Paul A. Colbert
Associate General Counsel
Regulatory Affairs

February 4, 2019

Hon. Kathleen H. Burgess
Secretary to the Commission
New York State Public Service Commission
Agency Building 3
Albany, NY 12223-1350

Re: Case 18-M-0376 - *Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place*, and Case 15-M-0180 - *In the Matter of Regulation and Oversight of Distributed Energy Resource Providers and Products;* Joint Utilities' Petition for Approval of the Business to Business Process Used to Formulate a Data Security Agreement and for Affirming the Joint Utilities' Authority to Require and Enforce Execution of the Data Security Agreement by Entities Seeking Access to Utility Customer Data or Utility Systems

Dear Secretary Burgess:

Pursuant to 16 NYCRR §§ 3.5 and 17.1, Central Hudson Gas & Electric Corporation ("Central Hudson"), Consolidated Edison Company of New York, Inc., National Fuel Gas Distribution Corporation, New York State Electric & Gas Corporation, Niagara Mohawk Power Corporation d/b/a National Grid, KeySpan Gas East Corporation d/b/a National Grid and The Brooklyn Union Gas Company d/b/a National Grid NY, Orange and Rockland Utilities, Inc., and Rochester Gas and Electric Corporation (collectively and individually, the "Joint Utilities") hereby submit this Petition for Approval of the Business to Business Process Used to Formulate a Data Security Agreement and for Affirming the Joint Utilities' Authority to Require and Enforce Execution of the Data Security Agreement by Entities Seeking Access to Utility Customer Data or Utility Systems.

284 South Avenue
Poughkeepsie, NY 12601

(845) 452-2000
Phone: (845) 486-5831 Cell: (614) 296-4779
Email: pcolbert@cenhud.com
www.CentralHudson.com

Please contact the undersigned at (845)486-5831 or pcolbert@cenhud.com with any questions regarding this matter.

Respectfully Submitted,

CENTRAL HUDSON GAS AND ELECTRIC CORPORATION
By: /s/ Paul A. Colbert
Paul A. Colbert
Associate General Counsel – Regulatory Affairs
Central Hudson Gas and Electric Corporation
284 South Avenue Poughkeepsie, NY 12601
Tel: (845) 486-5831
Email: pcolbert@cenhud.com

CONSOLIDATED EDISON COMPANY OF NEW YORK, INC. and ORANGE AND ROCKLAND UTILITIES, INC.
By: /s/ Kerri Kirschbaum
Kerri Kirschbaum
Associate Counsel
Mary Krayeske
Associate Counsel
Consolidated Edison Company of New York, Inc.
4 Irving Place
New York, New York 10003
Tel.: (212) 460-1077; (212) 460-1340
Email: kirschbaumk@coned.com
krayeskem@coned.com

NIAGARA MOHAWK POWER CORPORATION d/b/a NATIONAL GRID
By: /s/ Jeremy J. Euto
Jeremy J. Euto
Senior Counsel
National Grid
300 Erie Boulevard
West Syracuse, New York 13202

Tel: (315) 428-3310
Email: Jeremy.euto@nationalgrid.com

NEW YORK STATE ELECTRIC & GAS CORPORATION and ROCHESTER GAS AND ELECTRIC CORPORATION
By: /s/ Mark Marini
Mark Marini
Director - Regulatory
89 East Avenue
Rochester, NY 14649
Tel.: (585) 750-1666
Email: Mark_Marini@rge.com

NATIONAL FUEL GAS DISTRIBUTION CORPORATION
By: /s/ Ty A. Holt
Ty A. Holt, Esq.
Senior Attorney
Rates & Regulatory Affairs
6363 Main Street
Williamsville, NY 14221
Tel.: (716) 857-7735
Email: holtt1@natfuel.com

STATE OF NEW YORK
PUBLIC SERVICE COMMISSION

Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place.	Case 18-M-0376
In the Matter of Regulation and Oversight of Distributed Energy Resource Providers and Products	Case 15-M-0180

JOINT UTILITIES' PETITION FOR APPROVAL OF THE BUSINESS-TO-BUSINESS PROCESS USED TO FORMULATE A DATA SECURITY AGREEMENT AND FOR AFFIRMING THE JOINT UTILITIES' AUTHORITY TO REQUIRE AND ENFORCE EXECUTION OFTHE DATA SECURITY AGREEMENT BY ENTITIES SEEKING ACCESS TO UTILITY CUSTOMER DATA OR UTILITY SYSTEMS

Table of Contents

INTRODUCTION

Pursuant to 16 NYCRR §§ 3.5 and 17.1, the Joint Utilities[1] file this petition to assure that entities seeking access to customer data within utility systems provide sufficient protection for that access. Specifically, the Joint Utilities ask the New York State Public Service Commission ("Commission") to:

- Confirm that the business-to-business process among parties, the Joint Utilities, New York State Department of Public Service ("Staff"), Energy Service Companies ("ESCOs"), Distributed Energy Resource Suppliers ("DERS"), Direct Customers, and other entities, that was used to negotiate and develop a Data Security Agreement ("DSA") and its accompanying Self-Attestation ("SA")[2] to receive customer data through the interconnection to utility system was appropriate for development of the DSA;
- Authorize the amendment of the DSA going forward through the business to business process which should include at a minimum, standard requirements that: (1) specify compliance with the Uniform Business Practices ("UBP"), UBP DERS, or other applicable Commission rules; (2) address the transfer of information; (3) maintain the confidentiality of Joint Utilities and the ESCOs, DERS, Direct Customers, and their applicable contractors (collectively, "Energy Service Entities" or "ESEs") information, including the protection of customer data; (4) requiring the

[1] The Joint Utilities are (collectively and individually) Central Hudson Gas & Electric Corporation ("Central Hudson"), Consolidated Edison Company of New York, Inc., National Fuel Gas Distribution Corporation, New York State Electric & Gas Corporation, Niagara Mohawk Power Corporation d/b/a National Grid, KeySpan Gas East Corporation d/b/a National Grid and The Brooklyn Union Gas Company d/b/a National Grid NY, Orange and Rockland Utilities, Inc., and Rochester Gas and Electric Corporation.

[2] In this Petition, the term DSA means executing the DSA and submitting a satisfactory SA. The document is attached as Petition Attachment 1.

return and destruction of information; (5) address each Party's responsibility and liability for data security incidents; (6) require cyber security insurance; (7) define minimum cyber security requirements; (8) address how to determine whether ESEs have and maintain minimum levels of cyber security; and (9) require ESE indemnification of the Joint Utilities; and

- Affirm the Joint Utilities' authority to require ESEs to satisfactorily complete a DSA, which will evolve in the future, and prohibit ESEs[3] from electronic access to utility information technology ("IT") systems as well as customer data without a DSA.

As shown below, the Joint Utilities seek Commission approval of the business-to-business process used to develop the DSA because some ESEs claim that a rulemaking process must precede the Joint Utilities requiring that ESEs execute the DSA.[4] The business-to-business process, however, was a lengthy and publicly noticed proceeding, as described below, and provided a full opportunity for all parties to participate.[5] The Joint Utilities emphasize that they are requesting that the Commission approve the process that resulted in the document as well as the framework for the document, not necessarily the specific underlying documents, as the Joint Utilities expect that the DSA will need to be modified as technology and cyber security standards evolve.

---

[3] As this relates to ESCOs, the Joint Utilities filed a *Petition of the Joint Utilities for Declaratory Ruling Regarding their Authority to Discontinue Utility Access to Energy Services Companies in Violation of the Uniform Business Practices* on November 9, 2018 in Cases 98-M-1343 and 18-M-0376 (ESCO Declaratory Ruling Petition) (attached as Petition Attachment 2). This Petition seeks similar treatment of for ESEs, Direct Customers and other current and future entities as it relates to customer information. The Joint Utilities expect that the ESCO Declaratory Ruling Petition will be subsumed into this request. Operations system interconnections between the utilities and DERS are not included or discussed under this Petition and will require different and more stringent security standards.

[4] See Comment 19 at Petition Attachment 3 (Petition Attachment 3 summarizes DERS' comments filed in Case 18-M-0376).

[5] *See* Case 18-M-0376 - *Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place* (Department of Public Service Staff Report on the Status of the Business-To-Business Collaborative to Address Cyber Security in the Retail Access Industry at 3) (September 24, 2018).

In addition, the Joint Utilities request that the Commission affirm their authority to require the ESEs to execute a DSA and to prohibit ESEs that fail to do so from obtaining data from or access to the applicable utility's IT systems. Pursuant to the UBP and UBP DERS, the Joint Utilities have authority to require ESEs to execute a DSA and have the right to prohibit non-compliant ESEs from accessing customer data and utility IT systems. The Joint Utilities would note that the ESEs should be treated as any other vendor, i.e., ESEs should be required to meet the Joint Utilities terms and conditions, which would include cyber security terms, as the Joint Utilities have the right to set and negotiate transactional terms and conditions independently.

The relief requested in this Petition addresses other related pending petitions and proceedings. In addition to the ESCO Declaratory Ruling Petition, this Petition addresses the Joint Utilities' November 21, 2017 Request for Clarification in the DERS Oversight Proceeding,[6] a copy of which is attached as Petition Attachment 4, as well as the Petition for Declaratory Ruling submitted on December 4, 2018 by Mission:data Coalition ("Mission:data")[7] to which the Joint Utilities response is attached as Petition Attachment 5.[8] The Request for Clarification and Mission:data Petition both address whether the Joint Utilities can require DERS to comply with cyber security requirements, including signing the DSA. Finally, a ruling on this Petition will inform the upcoming comprehensive

[6] Case 15-M-0180, *In the Matter of Regulation and Oversight of Distributed Energy Resource Providers and Products*, Joint Utility Request for Clarification (November 21, 2017).
[7] Case 18-M-0376, *Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place* ("Cyber Security Proceeding"), Petition for Declaratory Ruling (November 30, 2018).
[8] Cyber Security Proceeding, Joint Utility Response to Petition for Declaratory Ruling (December 21, 2018).

proceeding on customer data access initiated in the Commission's December 13, 2018 *Order Adopting Accelerated Energy Efficiency Targets*.[9]

The Joint Utilities support the Commission's effort to develop competitive markets, including those involving ESEs. However, those markets must develop in tandem with maintaining the security of customer data and utility IT systems through appropriate cyber security measures. This means that each market participant must bear the cost responsibility of its IT systems and customers without shifting cost responsibility to non-participating customers or entities. Moreover, entities must be required to responsibly participate in the market by safeguarding confidential data, particularly customer data, and the Joint Utilities' IT systems.

Although ESEs agree that all entities should maintain adequate cyber security, some protest the DSA's reasonable and minimal data privacy and cyber security standards. While many ESEs have executed the DSA, others refuse absent a Commission determination. The Joint Utilities assert that they have the authority to require execution of DSAs without Commission approval, but have submitted this petition to confirm their right to do so.

BACKGROUND

Cyber security is not a theoretical problem. It is a real problem facing the Joint Utilities, ESEs, and customers. The Joint Utilities face the constant risk of cyber-attacks and consequently, maintain cyber security defenses. If these defenses fail, the utility

[9] Case 18-M-0084, *In the Matter of a Comprehensive Energy Efficiency Initiative*, Order Adopting Accelerated Energy Efficiency Targets, December 13, 2018 ("NE:NY Order"). The Joint Utilities would note that deferring this matter to that new proceeding is inappropriate as this matter has been pending for almost a year and the Joint Utilities understand that the NE;NY proceeding is meant to be an on-going collaborative to address data issues.

could suffer a cyber security incident and its effects, including significant costs, and regulatory and reputational issues.[10] ESEs similarly must maintain adequate cyber security to protect customer data and to secure business processes. Cyber protections are weakened, and risks increase, when one party to an electronic interaction fails to maintain adequate security.

Specifically, utilities face significant risk from outsiders trying to enter their systems. Cyber security bad actors look to attack what they perceive to be the weakest link, those that contract with utilities, because contractors often do not have strong cyber security measures in place.[11] In 2017, a cyber security attack was implemented using utility vendors against United States utilities by a nation state actor.[12] The attack included New York entities, including utilities.[13]

Attacks come from all sorts of entities with varied goals. The Joint Utilities constantly experience attacks on their cyber security systems and attempts to access customer data. Bad actors collect data from wherever they can to commit crimes against customers.[14] Absent a requirement that ESEs enact reasonable cyber security measures, the likelihood of a major cyber security event affecting New York utilities increases.

[10] Similarly, New York State Law requires State agencies to adhere to the New York State Information Technology Policies and Standards administered by the New York State Office of Information Technology Services ("NYITS").
[11] The Wall Street Journal (America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It) (January 10, 2019) (Petition Attachment 6).
[12] *Id*.
[13] *Id*.
[14] For example, Central Hudson is aware of scams committed against 65 ESCO customers during 2018.

The Joint Utilities request that ESEs maintain a minimum level of protection, not a higher level of protection required for vendors and contractors.[15] The costs of implementing reasonable cyber security controls significantly outweigh the risks associated with not having adequate controls.[16] The cost of a cyber security incident averaged more than $17 million for financial service, utility, and energy companies in 2017,[17] a 22.7 percent increase over the 2016 cost.[18] The number of cyber security incidents continues to rise each year.[19] Deployed cyber security measures result in cost savings and increased return on investment when compared to the expected cost of a cyber security incident.[20]

Utilities must protect against this threat, including vigilance regarding their own security, as well as by requiring protection from entities that either do business with utilities, have utility data, including customer information, or have any connection to the utility system. This is true regardless of the type of entity—whether DERS, ESCO, Direct Customer, or other third party.

The Commission has a long history of protecting customer data and requiring cyber security. In 2010, the Commission stated that "[p]rotection of consumer information is a basic tenet of the Public Service Law and our policies."[21] The Commission approved a contract between Central Hudson and its vendor, OPower, in part, because the

[15] The Joint Utilities believe that ESEs should have a higher level of cyber security but, at this time, are willing to accept the terms and conditions included in the SA.
[16] *See Cost of Compliance With Data Protection Regulations* at 10 (Poneman Institute LLC) (December 2017) (Petition Attachment 7 at 11).
[17] 2017 Cost of Cyber Crime Study at 3 (Ponemon Institute LLC) (Petition Attachment 8).
[18] *Id*.
[19] *Id*.
[20] *Id*. at 34-35.
[21] Cases 07-M-0548 et al., *Proceeding on Motion of the Commission Regarding an Energy Efficiency Portfolio Standard* ("EEPS Proceeding"), (Order on Rehearing Granting Petition for Rehearing at 17) (issued and effective December 3, 2010) ("OPower Order").

agreement included "privacy safeguards," which prohibited OPower from using customer information and usage data for any purpose other than to administer the program.[22] The Commission also noted with approval that the agreement included indemnification provisions in the utility's favor in the event of a breach or non-compliance of the agreement,[23] and cyber security standards; specifically, the National Institute of Standards and Technology ("NIST").[24]

In initiating the Reforming the Energy Vision ("REV") proceeding, the Commission re-emphasized the need for cyber security, finding that "[c]yber security is highly important for reasons of privacy, reliability, resiliency and market confidence."[25] The Commission also noted that technology is evolving and as a result, this area will require constant vigilance.[26] In its *Order Adopting Distributed System Implementation Plan Guidance*, the Commission again emphasized the importance of cyber security,[27] and regarding interconnections between utilities and DERS decided that "[a]long with identification of new system tools, rules must be put in place *incorporating cybersecurity and privacy protection*."[28]

In the *Order Instituting Proceeding* in the Cyber Security Proceeding,[29] the Commission raised concerns about a recent retail market cyber incident and recognized

[22] *Id*. at 17-18 (emphasis added).
[23] *Id.*
[24] *Id*. at 14.
[25] Case 14-M-0101 - *Proceeding on Motion of the Commission in Regard to Reforming the Energy Vision* ("REV Proceeding"), Order Adopting Regulatory Policy Framework and Implementation Plan at 99, (Issued February 26, 2015) (citing Report: Cyber Attacks Likely to Increase, Rainie, Lee; Anderson, Janna; and Connolly, Jennifer, Pew Research Internet Project, October 29, 2014).
[26] *Id*. at 100.
[27] REV Proceeding, *Order Adopting Distributed System Implementation Plan Guidance* at 2-3, (issued April 20, 2016).
[28] *Id*. at 14 (emphasis added).
[29] Cyber Security Proceeding, Order Instituting Proceeding (issued June 14, 2018).

that cyber security threats are becoming more common and that industry must be vigilant in order to protect against, detect, and respond to these events. The Commission went on to state: "[i]t is essential to ensure that cyber security protections are being adequately addressed to mitigate vulnerability of utility systems to cyber-attacks, and to ensure that confidential and sensitive customer information remains safeguarded from potential data breaches."[30]

Most recently, in the NE:NY Order, the Commission reasserted the need for appropriate safeguards when the utility shares data. For example, relating to energy efficiency providers acting as utility contractors, the Commission stated that there should be "safeguards [that] ensure that data provided to third-party contractors is only used for implementing utility programs and that appropriate security and privacy protections are in place."[31]

PROCEDURAL HISTORY

In March 2018, a provider of electronic data interchange ("EDI") services to many ESCOs had a cyber security event that affected the ESCOs with which it had a contractual relationship. This event exposed the utilities (including the Joint Utilities) with which the ESCOs did business, and their customers, to additional cyber risk. Many of the Joint Utilities were not notified of the cyber security incident until several weeks after the event.[32] Once the Joint Utilities learned that a cyber security incident had occurred, to protect their IT systems, they immediately ceased electronic communication with the entity, advised Staff of the issue, and attempted to work with affected ESCOs.

[30] *Id.* at 3.
[31] NE:NY Order at 43.
[32] Several weeks after the cyber security incident occurred, in April 2018, the entity finally confirmed the incident to non-contracted utilities.

Before reauthorizing transactions with the entity, the impacted Joint Utilities required the entity to: (1) provide information on the security of its system, (2) conduct retesting, and (3) enter an agreement requiring the entity to undertake cyber security measures, including providing assurance of cyber security insurance coverage. During this time, the Joint Utilities constantly communicated with Staff and ESCOs. Impacted Joint Utilities restored service with reasonable, although temporary, cyber security measures in place. At the same time, the Joint Utilities requested that each ESCO doing business in each utility service territory enter a DSA with each Joint Utilities member.

Many ESEs initially objected to the proposed DSA. The proposed DSA was based upon the Commission-approved DSA for Community Choice Aggregation ("CCA") programs[33] and additionally included: (1) a requirement for cyber insurance, (2) a data security rider detailing cyber security requirements for each Joint Utility, and (3) for some of the Joint Utilities, a vendor questionnaire concerning the state of the ESE's cyber security. To facilitate implementation of the DSA, along with the ESEs and Staff, the Joint Utilities began a business-to-business process to formulate an acceptable DSA.

After initial discussions, Staff hosted a publicly noticed technical conference at the Commission's offices on May 31, 2018, where the Joint Utilities explained the need for the DSA. In response to the ESEs comments, the Joint Utilities reformulated the five separate data security riders and vendor questionnaire into one uniform SA that they circulated to the ESEs by June 8, 2018, and which the ESEs were asked to submit by June 30, 2018. The SA represented a significant compromise for the Joint Utilities

[33] Case 14-M-0224, *Proceeding on Motion of the Commission to Enable Community Choice Aggregation Program*, Order Approving Community Choice Aggregation Program and Utility Data Security Agreement with Modifications (Issued October 19, 2017).

because it applied a less rigorous cyber security evaluation for the ESEs than initially proposed.[34] At the same time, the Joint Utilities revised the DSA, which the ESEs were to sign by July 31, 2018.

On June 14, 2018, the Commission issued its *Order Instituting Proceeding* in the Cyber Security Proceeding. This Order expressly supported the on-going business-to-business process between the Joint Utilities and ESEs, recognized the common occurrence of cyber security events and the need for cyber security, and directed Staff to monitor the business-to-business process and file a report on the status of discussions among the parties by August 31, 2018.[35]

The business-to-business process continued with teleconferences, in-person meetings—including two in-person meetings in late July—and the exchange of written comments. The Joint Utilities amended terms in the DSA, responding to the ESEs' concerns. The Joint Utilities asked for the ESEs to submit SAs by August 24, 2018 and execute the final DSA, which was sent to the ESEs on August 16, 2018, by August 31, 2018. As they stated at July 26-27 in-person meeting, the Joint Utilities stated their intention to continue to participate in a collaborative working group with ESEs to discuss and amend the DSA as necessary to meet evolving cyber security requirements.

Most ESCOs, serving over 90 percent of New York's mass market choice customers, submitted signed DSAs, although some did so under protest. Other ESEs have not submitted a DSA.

[34] It is critical to note that a utility requires vendors with which it contracts to abide by more stringent cyber security protections. If a utility contracted with an ESE, the utility would require the stronger cyber security protections.
[35] *Id*. at 2.

On September 24, 2018,[36] Staff filed its report that found that the standardized SA required a minimal level of cyber security compliance, the DSA was "balanced," and the business-to-business process should continue with DERS to increase participation.[37] Thereafter, to address the non-compliant ESEs, the Joint Utilities filed the ESCO Declaratory Ruling Petition on November 9, 2018.

As requested by the Staff Report, on November 14, 2018, the DERS, Joint Utilities, and Staff continued the business-to-business process in person. Some DERS complained about the need for a DSA but presented no information to distinguish them from other ESEs. The Joint Utilities, DERS, and Staff agreed that DERS would file written comments detailing their specific concerns with the DSA by December 14, 2018.[38]

In the meantime, on November 30, 2018, Mission:data filed its Petition for Declaratory Ruling seeking to exempt DERS from cyber security requirements.[39] On December 21, 2018, the Joint Utilities submitted a response opposing Mission:data's Petition.

There have been many comments, oral and written, submitted during the business-to-business process to develop the DSA. During the initial discussions between the Joint Utilities, Staff, and primarily ESCOs and EDI providers, many commenters objected to the cyber security proposed in the DSA and to the provision of cyber security insurance.

---

[36] *Id*. (Department of Public Service Staff Report on the Status of the Business-To-Business Collaborative to Address Cyber Security in the Retail Access Industry) (September 24, 2018). Staff received an extension from the Secretary for this filing (August 24, 2018).
[37] *Id*. at 8.
[38] Six sets of comments by DERS were filed regarding the SA and DSA by DERS. The Joint Utilities respond to the comments in Attachment A.
[39] Case 18-M-0376 - *Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place* (Petition of Mission:data Coalition for Declaratory Ruling Regarding the DER Oversight Order's Exemption of DER Suppliers from Certain Cybersecurity Requirements) (November 30, 2018). The Joint Utilities and others responded to the Mission;data's Petition on December 21, 2018.

Also at the November 14, 2018 meeting, Mission:data's presentation opined, incorrectly and without evidence, that no other State was applying cyber security requirements as stringent as those proposed by the Joint Utilities for Green Button Connect.[40] Meeting participants were specifically asked to identify any facts and risk mitigation that might distinguish DERS from ESCOs and other ESEs, but no information was offered to show that the electronic interaction between the Joint Utilities and DERS was less risky than the electronic interaction with other ESEs. Similarly, no such information was offered in the written comments summarized and addressed in Attachment 2.

Six entities filed comments and advanced nearly 30 different arguments to support their positions regarding the proposed DSA. The comments suggested that the DSA, or specific provisions therein, be eliminated or made inapplicable to DERS or otherwise weakened to eliminate the DERS' burden of cyber security compliance and to shift the risk of cyber security costs and incidents to both customers and the Joint Utilities.

DISCUSSION

The Joint Utilities have addressed cyber security for many years, including review and enhancement of cyber security protections for their own systems as technology evolves, and the purchase and maintenance of cyber security insurance. Not only have the Joint Utilities addressed their own cyber security, they have routinely required their contractual counterparties with whom they have electronic interactions (other than by email) or who receive confidential customer information to comply with cyber security measures. Due to the Joint Utilities' requirements the cyber security measures required

[40] The Joint Utilities' positions are also fully explained in their Mission:data response, attached as Petition Attachment 5.

of counterparties have evolved to be consistent with cyber security best practices, including the provision of cyber insurance.

During the evolution of cyber security measures, the Joint Utilities have held discussions with stakeholders about the applicability of those measures to competitive entities including ESCOs, DERS, and Direct Customers since, in many instances, the relationship between the Joint Utilities and these entities, especially ESCOs, predate today's cyber security issues.

Despite almost a year of working to address protecting customer data and utility IT systems, during which the Joint Utilities have made significant compromises to meet ESEs' concerns, some ESE's have either not submitted the DSA and/or demanded a Commission Order mandating the DSA.

As noted above, developing commodity, renewable, and energy efficiency markets is an important goal. As part of that goal, however, all market participants must be treated as a business and must bear the costs associated with that business. As described above, the Joint Utilities do not contract with vendors that do not meet their required cyber security terms. Yet, the ESEs have not demonstrated any reason that they should receive different treatment. In fact, their only justification to be relieved of responsibility for their business risk seems to be that they should not have to bear these costs, an argument that shifts their costs to others and is unreasonable for every other entity that transacts business in today's cyber-focused world.

I. ESEs Must Implement and Maintain Adequate Cyber Security

ESEs continually have stated that adequate cyber security should be in place to protect customer data and IT systems. But the ESEs opine that the DSA should be

rejected because cyber security compliance costs too much or that there has not been an adequate process to develop the DSA.

The argument that the ESEs should not have to invest in cyber security because it will slow market development displays a misunderstanding of the cyber security issue. Developing a market without cyber security compliance will lead to cyber security issues, future compliance costs, and potential significant costs for a cyber security incident. No entity is immune to a cyber security event and the customer information ESEs receive from utilities and the entities' connection to utility IT systems puts customers and the Joint Utilities at risk from a cyber security event caused by an ESE. Given this fact, developing a market without these important protections will only lead to future problems and unreasonable cost shifts.

The DSA, described by the Staff Report as "balanced," represents the minimum level of security that the ESEs should have. Without this security, ESEs should not be permitted to connect to utility systems or, critically, receive customer data. As discussed more fully in the Joint Utilities' response to Mission:data's Petition, the requirements in the DSA align with the cyber security and customer data privacy requirements of other states.

As shown in detail in the Procedural History above and addressed in Petition Attachment 3 at comment 19, a robust and substantial process supported the development of the DSA. The process included multiple meetings to refine the DSA. As the Joint Utilities have previously explained, we believe this supports our adoption of the DSA without the need for additional process. Nevertheless, so that the Commission can confirm the DSA requirement, the Joint Utilities filed this petition, which will result in

publication of a notice in the State Register and the opportunity for parties to provide comments pursuant to that notice.

II. Utilities Have Authority to Require the DSA and Discontinue ESE Participation in Utility Programs in the Absence of an Executed DSA

ESEs, and particularly DERS, claim that they need not implement and maintain cyber security measures for a variety of reasons, including the cost of implementation or that there should be different requirements based on the platform they are retrieving data from or the type of services they provide to customers. Some ESE's and stakeholders, like Mission:data, believe that the DERS UBPs do not allow the Joint Utilities to protect their systems or customer data in any way. All of these arguments are incorrect. The Joint Utilities' response to the Mission:data Petition provides a detailed response to these arguments made by ESEs and is incorporated herein by reference.

As fully explained in the Joint Utilities' response to Mission:data, the UBP DERS Order affirmatively applied UBP-DERS Section 2(C) to EDI transactions between DERS and utilities.[41] The Commission, nonetheless, recognized that there are other methods and platforms for sharing customer data, and that the requirements and policies, including cyber security and customer data protections, associated with receiving data through these systems "will be developed in those venues."[42]

Until the Commission develops methods to regulate other methods and platforms, the Commission stated:

> Rules governing behavior in and oversight of those programs and transactions will appear within the program rules, the utility tariff, *or the procurement request or contract*,

[41] CASE 15-M-0180 - *In the Matter of Regulation and Oversight of Distributed Energy Resource Providers and Products* (Order Establishing Oversight Framework and Uniform Business Practices for Distributed Energy Resource Suppliers at 18, 28) (Issued and Effective: October 19, 2017) ("UBP DERS Order").
[42] *Id*. at 28.

> though the Commission may consider standardization of such rules into the UBP-DERS in the future.[43]

Based on this statement, a utility may require a DSA with DERS even if they are not engaged in EDI transactions with a utility and subject to the UBP DERS. Moreover, contrary to the assertions made by Mission:Data and others, nothing in the DERS UBPs prohibits the Joint Utilities from imposing any requirements for third party access to Green Button Connect. The fact that the UBP-DERs have a section establishing requirements for DERs using EDI does not mean that DERs using other platforms can do so without any requirements.

The Joint Utilities assert that the following DERS UBP rule applies to all DERS, regardless of the platform they are using to obtain customer-specific data:

"Data Security. DER suppliers that obtain customer information from the distribution utility or DSP must comply with any data security requirements imposed by that utility or by Commission rules on ESCOs and/or any data security requirements associated with EDI eligibility."[44] Further, as it relates to ESCOs or Direct Customers, UBP Section 2(F)(1)(a) expressly permits a utility to discontinue an ESCO or Direct Customer's participation in their Retail Access Program if the ESCO or Direct Customer's:

> Failure to act that is likely to cause, or has caused, *a significant risk or condition that compromises the safety, system security*, or operational reliability of the distribution utility 's system, and the ESCO or Direct Customer failed to eliminate immediately the risk or condition upon verified receipt of a non-EDI notice;…[45]

[43] *Id*. at 18 (emphasis added).
[44] UBP DERS Section 2(C)(G). This issue was previously raised in the Joint Utilities November 21, 2017 Request for Clarification.
[45] UBP at § 2(F)(1)(a) (emphasis added).

Thus, the Joint Utilities have the right to impose the DSA on ESEs and the Commission should confirm that right in its order on this petition.

CONCLUSION

For the reasons fully discussed above, the Joint Utilities urge the Commission to grant the relief requested as necessary to maintain minimum cyber security standards that have been established through the business-to-business process adopted by the Commission in this proceeding and as necessary to fully protect the interests of customer data privacy and utility cyber security. The Joint Utilities should be permitted to appropriately protect themselves and not be mandated to knowingly provide information or IT system access to an entity that does not have appropriate cyber controls.

ESEs' execution of the DSA is a practical and effective way to establish and implement minimum cyber security controls. The Joint Utilities' believe that the process to bring ESEs and the Joint Utilities current with industry cyber security standards has been robust and fair and they have the right to require DSAs. Nevertheless, the Joint Utilities file this Petition to address the non-participating ESEs' that have refused to execute DSAs and speed the effort to put necessary customer and utility protections in place.

Accordingly, the Joint Utilities request that the Commission: (1) approve the continuing business-to-business process to develop and implement a DSA to protect customer information and utility IT systems; (2) approve minimum standard requirements in the DSA subject to the continuing evolution of the DSA; and (3) affirm the Joint Utilities' existing authority to require ESEs to submit and execute a DSA and, if they fail to do so, disconnect them from the utility's IT systems and remove their access to customer information in order to protect customers and utilities from a potential cyber security event.

Given the importance of maintaining proper cyber security controls, the Joint Utilities urge the Commission to act expeditiously in addressing this Petition.

Respectfully submitted by:

CENTRAL HUDSON GAS AND ELECTRIC CORPORATION
By: /s/ Paul A. Colbert
Paul A. Colbert
Associate General Counsel – Regulatory Affairs
Central Hudson Gas and Electric Corporation
284 South Avenue Poughkeepsie, NY 12601
Tel: (845) 486-5831
Email: pcolbert@cenhud.com

CONSOLIDATED EDISON COMPANY OF NEW YORK, INC. and ORANGE AND ROCKLAND UTILITIES, INC.
By: /s/ Kerri Kirschbaum
Kerri Kirschbaum
Associate Counsel
Mary Krayeske
Associate Counsel
Consolidated Edison Company of New York, Inc.
4 Irving Place
New York, New York 10003
Tel.: (212) 460-1077; (212) 460-1340
Email: kirschbaumk@coned.com
krayeskem@coned.com

NIAGARA MOHAWK POWER CORPORATION d/b/a NATIONAL GRID
By: /s/ Jeremy J. Euto
Jeremy J. Euto
Senior Counsel
National Grid
300 Erie Boulevard
West Syracuse, New York 13202
Tel: (315) 428-3310
Email: Jeremy.euto@nationalgrid.com

NEW YORK STATE ELECTRIC & GAS CORPORATION and ROCHESTER GAS AND ELECTRIC CORPORATION
By: /s/ Mark Marini
Mark Marini
Director - Regulatory
89 East Avenue
Rochester, NY 14649
Tel.: (585) 750-1666
Email: Mark_Marini@rge.com

NATIONAL FUEL GAS DISTRIBUTION CORPORATION
By: /s/ Ty A. Holt
Ty A. Holt, Esq.
Senior Attorney
Rates & Regulatory Affairs
6363 Main Street
Williamsville, NY 14221
Tel.: (716) 857-7735
Email: holtt1@natfuel.com

DATA SECURITY AGREEMENT

This Data Security Agreement ("Agreement") effective _____, is made and entered into this _____ day of _____ , 20___ by and between ("Utility") and _____, an Energy Service Entity ("ESE") with offices at _____; and together with Utility the ("Parties" and each, individually, a "Party").

RECITALS

WHEREAS, ESE desires to have access to certain utility customer information, either customer-specific or aggregated customer information, or the New York State Public Commission ("Commission") has ordered Utility to provide to ESE customer information; and

WHEREAS, ESE has obtained consent from all customers from whom the ESE intends to obtain information from Utility; and

WHEREAS, Energy Services Company ("ESCO"), Direct Customer or Distributed Energy Resource ("DER") Supplier may utilize a third party to fulfill its Service obligations, including but not limited to, Electronic Data Interchange ("EDI") communications with Utility; and

WHEREAS, ESCO, Direct Customer or DER Supplier ("DERS") utilization of a third party provider does not relieve ESCO, Direct Customer or DERS of their transactional obligation such that they must ensure that the third party provider must comply with all ESCO, Direct Customer or DERS obligations; and

WHEREAS, Utility and ESE also desire to enter into this Agreement to establish, among other things, the full scope of ESE's obligations of security and confidentiality with respect to the Confidential Information in a manner consistent with the rules and regulations of the Commission and requirements of Utility; and

NOW, THEREFORE, in consideration of the premises and of the covenants herein contained, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties, intending to be legally bound, hereby agree as follows:

1. Definitions.

a. "Confidential ESE Information" means information that ESE is: (A) required by the Uniform Business Practices ("UBP") or DERS UBP ("UBP DERS") to receive from the end use customer and provide to Utility to enroll the customer or (B) any other information provided by ESE to Utility and marked confidential by the ESE, but excludes (i) information which is or becomes generally available to the public other than as a result of a disclosure by Receiving Party or its Representatives; (ii) information which was already known to Receiving Party on a non-confidential basis prior to being furnished to Receiving Party by Disclosing Party; (iii) information which becomes available to Receiving Party on a non-confidential basis from a source other than Disclosing Party or a representative of Disclosing Party if such source was not subject to any

prohibition against transmitting the information to Receiving Party and was not bound by a confidentiality agreement with Disclosing Party; (iv) information which was independently developed by the Receiving Party or its Representatives without reference to, or consideration of, the Confidential Information; or (v) information provided by the customer with customer consent where the customer expressly agrees that the information is public.

b. "Confidential Utility Information" means information that Utility is: (A) required by the UBP at Section 4: Customer information(C)(2), (3) or UBP DERS at Section 2C: Customer Data, to provide to ESCO, Direct Customer or DERS or (B) any other information provided to ESE by Utility and marked confidential by the Utility at the time of disclosure, but excludes (i) information which is or becomes generally available to the public other than as a result of a disclosure by Receiving Party or its Representatives; (ii) information which was already known to Receiving Party on a non-confidential basis prior to being furnished to Receiving Party by Disclosing Party; (iii) information which becomes available to Receiving Party on a non-confidential basis from a source other than Disclosing Party or a representative of Disclosing Party if such source was not subject to any prohibition against transmitting the information to Receiving Party and was not bound by a confidentiality agreement with Disclosing Party; (iv) information which was independently developed by the Receiving Party or its Representatives without reference to, or consideration of, the Confidential Information; or (v) information provided by the customer with customer consent where the customer expressly agrees that the information is public.

c. "Confidential Information" means, collectively, Confidential Utility Information or Confidential ESE Information.

d. "Data Protection Requirements" means, collectively, (A) all national, state, and local laws, regulations, or other government standards relating to the protection of information that identifies or can be used to identify an individual that apply with respect to ESE or its Representative's Processing of Confidential Utility Information; (B) industry best practices or frameworks to secure information, computer systems, network, and devices using a defense-in-depth approach, such as and including, but not limited to, NIST SP 800-53, ISO 27001 / 27002, COBIT, CIS Security Benchmarks, Top 20 Critical Controls as best industry practices and frameworks may evolve over time; and (C) the Commission rules, regulations, and guidelines relating to confidential data, including the Commission-approved UBP and UBP DERS.

e. "Data Security Incident" means a situation when Utility or ESE reasonably believes that there has been: (A) the loss or misuse (by any means) of Confidential Information; (B) the unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of Confidential Information, or Private Information as defined by GBL § 899-aa, computer systems, network and devices used by a business; (C) any other act or omission that compromises the security, confidentiality, or integrity of Confidential Information, or (D) any material breach of any Data Protection

Requirements in relation to the Processing of Confidential Information, including by any current or former Representatives.

f. "DER Supplier" or "DERS" has the meaning set forth in the UBP DERS approved by the Commission and as it may be amended from time to time, which is "[a] supplier of one or more DERs that participates in a Commission authorized and/or utility or DSP-operated program or market. DERS may choose to provide DERs as standalone products or services, or may choose to bundle them with energy commodity. CDG Providers and On-Site Mass Market DG Providers are included within the definition of DERS. Entities which sell both DERs and energy commodity are both DERS and ESCOs."

g. "Direct Customer" has the meaning set forth in the UBP approved by the Commission and as it may be amended from time to time, which is "An entity that purchases and schedules delivery of electricity or natural gas for its own consumption and not for resale. A customer with an aggregated minimum peak connected load of 1 MW to a designated zonal service point qualifies for direct purchase and scheduling of electricity provided the customer complies with NYISO requirements. A customer with annual usage of a minimum of 3,500 dekatherms of natural gas at a single service point qualifies for direct purchase and scheduling of natural gas."

h. "ESCO" has the meaning set forth in the UBP approved by the Commission and as it may be amended from time to time, which is "an entity eligible to sell electricity and/or natural gas to end-use customers using the transmission or distribution system of a utility."

i. "ESE" shall have the meaning set forth in the Recitals and for the avoidance of doubt, includes but is not limited to ESCOs, Direct Customers, DERS and contractors of such entities with which Utility electronically exchanges data other than by email and any other entities with which Utility electronically exchanges data other than by email or by a publicly available portal.

j. "PSC" or "Commission" shall have the meaning attributed to it in the Recitals.

k. "Processing" (including its cognate, "process") means any operation, action, error, omission, negligent act, or set of operations, actions, errors, omissions, or negligent acts that is performed using or upon Confidential Information or Utility Data, whether it be by physical, automatic or electronic means, including, without limitation, collection, recording, organization, storage, access, adaptation, alteration, retrieval, use, transfer, hosting, maintenance, handling, retrieval, consultation, use, disclosure, dissemination, exfiltration, taking, removing, copying, processing, making available, alignment, combination, blocking, deletion, erasure, or destruction.

l. "Third-Party Representatives" or "Representatives" means those agents acting on behalf of ESCOs, Direct Customers, or DERS that are contractors or subcontractors and that store, transmit or process Confidential Utility

Information. For the avoidance of doubt, Third-Party Representatives do not include ESEs and their members, directors, officers or employees who need to know Confidential Utility Information for the purposes of providing Services.

m. "Services" mean any assistance in the competitive markets provided by ESEs to end use customers or ESCOs, Direct Customers or DERS that also require interaction with a Utility, including but not limited to the electronic exchange of information with a Utility, and must be provided in accordance with the UBP or UBP DERS.

n. "Utility Data" means data held by Utility, whether produced in the normal course of business or at the request of ESE.

2. Scope of the Agreement. This Agreement shall govern security practices of ESEs that have electronic communications, other than email, with the Utility and security practices that apply to all Confidential Utility Information disclosed to ESE or to which ESE is given access by Utility, including all archival or back-up copies of the Confidential Utility Information held or maintained by ESE (or it its Representatives) and Confidential ESE Information. No financial information, other than billing information, will be provided pursuant to this Agreement. If any information is inadvertently sent to ESE or Utility, ESE or Utility will immediately notify the Utility/ESE and destroy any such information in the appropriate manner.

3. ESE Compliance with all Applicable Commission Uniform Business Practices. The Parties agree that the Commission's UBP and UBP DERS set forth rules governing the protection of Confidential Information and electronic exchange of information between the Parties, including but not limited to EDI.

_____ESCO, Direct Customer or DERS utilizes a Third-Party Representative as a vendor, agent or other entity to provide electronic exchange of information, other than by email, with Utility ESE and will require Third-Party Representative to abide by the applicable UBP or UBP DERS.

4. Customer Consent. The Parties agree that the UBP and UBP DERS govern an ESE's obligation to obtain informed consent from all customers about whom ESE requests data from Utility. The ESE agrees to comply with the UBP and UBP DERS on customer consent and the Utility's tariffs regarding customer consent.

5. Provision of Information. Utility agrees to provide to ESE or its Representatives, certain Confidential Utility Information, as requested, provided that: (A) ESE and its Representatives are in compliance with the terms of this Agreement in all material respects; (B) if required by Utility, ESE has provided and has required its Representatives to provide, to the satisfaction of Utility any Vendor Product/Service Security Assessments or self–attestations (attached hereto as Exhibit A) or such other risk assessment forms as Utility may require from time to time ("Assessment") and ESE will comply with the Utility Assessment requirements as approved by the Utility; (C) ESE (and its Representatives, as applicable) shall have and maintain throughout the term, systems and processes in place and as

detailed in the Assessment acceptable to Utility to protect system security and Confidential Utility Information; and; (D) ESE complies and shall require its Third-Party Representatives who process Confidential Information to comply with Utility's Assessment requirements as approved by the Utility. Provided the foregoing prerequisites have been satisfied, ESE shall be permitted access to Confidential Utility Information and/or Utility shall provide such Confidential Utility Information to ESE. Nothing in this Agreement will be interpreted or construed as granting either Party any license or other right under any patent, copyright, trademark, trade secret, or other proprietary right or any right to assert any lien over or right to withhold from the other Party any Data and/or Confidential Information of the other Party. Utility will comply with the security requirements set forth in its Assessment.

6. Confidentiality. ESE shall: (A) hold all Confidential Utility Information in strict confidence pursuant to the UBP or UBP DERS and Commission's orders; except as otherwise expressly permitted by Section 7 herein; (B) not disclose Confidential Utility Information to any Third-Party Representatives, or affiliates, except as set forth in Section 7(a) of this Agreement; (C) not Process Confidential Utility Information other than for the Services defined in the Recitals as authorized by this Agreement; (D) limit reproduction of Confidential Utility Information; (E) store Confidential Utility Information in a secure fashion at a secure location that is not accessible to any person or entity not authorized to receive the Confidential Utility Information under the provisions hereof; (F) otherwise use at least the same degree of care to avoid publication or dissemination of the Confidential Utility Information as ESE employs (or would employ) with respect to its own confidential information that it does not (or would not) desire to have published or disseminated, but in no event less than reasonable care; and (G) to the extent required by the Utility, each Representative with a need to know the Confidential Utility Information shall sign the Third-Party Representative Agreement set forth as Exhibit B to this Agreement. At all times, Utility shall have the right for cause to request reasonable further assurances that the foregoing restrictions and protections concerning Confidential Utility Information are being observed and ESE shall be obligated to promptly provide Utility with the requested assurances.

Utility shall: (A) hold all Confidential ESE Information in strict confidence; except as otherwise expressly permitted by Section 7 herein; (B) not disclose Confidential ESE Information to any other person or entity except as set forth in Section 7(a) of this Agreement; (C) not Process Confidential ESE Information other than for the Services defined in the Recitals as authorized by this Agreement; (D) limit reproduction of Confidential ESE Information; (E) store Confidential ESE Information in a secure fashion at a secure location that is not accessible to any person or entity not authorized to receive the Confidential ESE Information under the provisions hereof; (F) otherwise use at least the same degree of care to avoid publication or dissemination of the Confidential ESE Information as Utility employs (or would employ) with respect to its own confidential information that it does not (or would not) desire to have published or disseminated, but in no event less than reasonable care; and (G) to the extent required by ESE, each Representative with

a need to know the Confidential ESE Information shall sign the Third-Party Representative Agreement set forth as Exhibit B to this Agreement. At all times, ESE shall have the right for cause to request reasonable further assurances that the foregoing restrictions and protections concerning Confidential ESE Information are being observed and Utility shall be obligated to promptly provide ESE with the requested assurances.

This Section 6 supersedes prior non-disclosure agreements between the Parties pertaining to Confidential Information.

7. Exceptions Allowing ESE to Disclose Confidential Utility Information.

a. **Disclosure to Representatives**. Notwithstanding the provisions of Section 6 herein, the Parties may disclose Confidential Information to their Third-Party Representatives who have a legitimate need to know or use such Confidential Information for the purposes of providing Services in accordance with the UBP and UBP DERS, provided that each such Third-Party Representative first: (A) is advised by the disclosing Party of the sensitive and confidential nature of such Confidential Information; (B) agrees to comply with the provisions of this Agreement, provided that with respect to Third-Party Representatives and this subsection (B), such Third-Party Representatives must agree in writing to be bound by and observe the provisions of this Agreement as though such Third-Party Representatives were a Party/ESE; and (C) signs the Third-Party Representative Agreement. All such written Agreements with Third-Party Representatives shall include direct liability for the Third-Party Representatives towards Utility/ESE for breach thereof by the Third-Party Representatives, and a copy of such Agreement and each Third-Party Representative Agreement shall be made available to Utility/ESE upon request. Notwithstanding the foregoing, the Parties shall be liable for any act or omission of a Third-Party Representative, including without limitation, those acts or omissions that would constitute a breach of this Agreement.

b. **Disclosure if Legally Compelled**. Notwithstanding anything herein, in the event that a Party or any of its Third-Party Representatives receives notice that it has, will, or may become compelled, pursuant to applicable law or regulation or legal process to disclose any Confidential Information (whether by receipt of oral questions, interrogatories, requests for information or documents in legal proceedings, subpoenas, civil investigative demands, other similar processes, or otherwise), that Party shall, except to the extent prohibited by law, within one (1) business day, notify the other Party, orally and in writing, of the pending or threatened compulsion. To the extent lawfully allowable, the Parties shall have the right to consult and the Parties will cooperate, in advance of any disclosure, to undertake any lawfully permissible steps to reduce and/or minimize the extent of Confidential Information that must be disclosed. The Parties shall also have the right to seek an appropriate protective order or other remedy reducing and/or minimizing the extent of Confidential Information that must be disclosed. In any event, the Party and its Third-Party Representatives shall disclose only such Confidential Information which they are advised by legal

counsel that they are legally required to disclose in order to comply with such applicable law or regulation or legal process (as such may be affected by any protective order or other remedy obtained by the Party) and the Party and its Third-Party Representatives shall use all reasonable efforts to ensure that all Confidential Information that is so disclosed will be accorded confidential treatment.

8. Return/Destruction of Information. Within thirty (30) days after Utility's written demand, ESE shall (and shall cause its Third-Party Representatives to) cease to access and Process Confidential Utility Information and shall at the Utility's option: (A) return such Confidential Utility Information to Utility in such manner, format, and timeframe as reasonably requested by Utility or, if not so directed by Utility, (B) shred, permanently erase and delete, degauss or otherwise modify so as to make unreadable, unreconstructible and indecipherable ("Destroy") all copies of all Confidential Utility Information (including any and all extracts, compilations, studies, or other documents based upon, derived from, or containing Confidential Utility Information) that has come into ESE's or its Third-Party Representatives' possession, including Destroying Confidential Utility Information from all systems, records, archives, and backups of ESE and its Third-Party Representatives, and all subsequent access, use, and Processing of the Confidential Utility Information by ESE and its Third-Party Representatives shall cease provided any items required to be maintained by governmental administrative rule or law or necessary for legitimate business or legal needs will not be destroyed until permitted and will remain subject to confidentiality during the retention period. ESE agrees that upon a customer revocation of consent, ESE warrants that it will no longer access through Utility Confidential Utility Information and that it will Destroy any Confidential Utility Information in its or its Third-Party Representative's possession. Notwithstanding the foregoing, ESE and its Third-Party Representatives shall not be obligated to erase Confidential Utility Information contained in an archived computer system backup maintained in accordance with their respective security or disaster recovery procedures, provided that ESE and its Third-Party Representatives shall: (1) not have experienced an actual Data Security Incident; (2) maintain Data Security Protections to limit access to or recovery of Confidential Utility Information from such computer backup system and; (3) keep all such Confidential Utility Information confidential in accordance with this Agreement. ESE shall, upon request, certify to Utility that the destruction by ESE and its Third-Party Representatives required by this Section has occurred by (A) having a duly authorized officer of ESE complete, execute, and deliver to Utility a certification and (B) obtaining substantially similar certifications from its Third-Party Representatives and maintaining them on file. Compliance with this Section 8 shall not relieve ESE from compliance with the other provisions of this Agreement. The written demand to Destroy or return Confidential Utility Information pursuant to this Section may occur if the ESE has been decertified pursuant to the UBP or UBP DERS, the Utility has been notified of a potential or actual Data Security Incident and Utility has a reasonable belief of potential ongoing harm or the Confidential Utility Information has been held for a period in excess of its retention period. The obligations under this Section shall survive any expiration of termination of this

Agreement. Subject to applicable federal, state and local laws, rules, regulations and orders, at ESE's written demand and termination of electronic exchange of data with Utility, Utility will Destroy or return, at ESE's option, Confidential ESE Information.

9. Audit. Upon thirty (30) days notice to ESE, ESE shall, and shall require its Third-Party Representatives to permit Utility, its auditors, designated representatives, to audit and inspect, at Utility's sole expense (except as otherwise provided in this Agreement), and provided that the audit may occur no more often than once per twelve (12) month period (unless otherwise required by Utility's regulators). The audit may include (A) the facilities of ESE and ESE's Third-Party Representatives where Confidential Utility Information is Processed by or on behalf of ESE; (B) any computerized or paper systems used to Process Confidential Utility Information; and (C) ESE's security practices and procedures, facilities, resources, plans, procedures, and books and records relating to the privacy and security of Confidential Utility Information. Such audit rights shall be limited to verifying ESE's compliance with this Agreement, including all applicable Data Protection Requirements. If the ESE provides a SOC II report or its equivalent to the Utility, or commits to complete an independent third-party audit of ESE's compliance with this Agreement acceptable to the Utility at ESE's sole expense, within one hundred eighty (180) days, no Utility audit is necessary absent a Data Security Incident. Any audit must be subject to confidentiality and non-disclosure requirements set forth in Section 6 of this Agreement. Utility shall provide ESE with a report of its findings as a result of any audit carried out by or on behalf of Utility. ESE shall, within thirty (30) days, or within a reasonable time period agreed upon in writing between the ESE and Utility, correct any deficiencies identified by Utility, and provide the SOC II audit report or its equivalent or the report produced by the independent auditor to the Utility and provide a report regarding the timing and correction of identified deficiencies to the Utility.

10. Investigation. Upon notice to ESE, ESE shall assist and support Utility in the event of an investigation by any regulator or similar authority, if and to the extent that such investigation relates to Confidential Utility Information Processed by ESE on behalf of Utility. Such assistance shall be at Utility's sole expense, except where such investigation was required due to the acts or omissions of ESE or its Representatives, in which case such assistance shall be at ESE's sole expense.

11. Data Security Incidents. ESE is responsible for any and all Data Security Incidents involving Confidential Utility Information that is Processed by, or on behalf of, ESE. ESE shall notify Utility in writing immediately (and in any event within forty-eight (48) hours) whenever ESE reasonably believes that there has been a Data Security Incident. After providing such notice, ESE will investigate the Data Security Incident, and immediately take all necessary steps to eliminate or contain any exposure of Confidential Utility Information and keep Utility advised of the status of such Data Security Incident and all matters related thereto. ESE further agrees to provide, at ESE's sole cost: (1) reasonable assistance and cooperation requested by Utility and/or Utility's designated representatives, in the

furtherance of any correction, remediation, or investigation of any such Data Security Incident; (2) and/or the mitigation of any damage, including any notification required by law or that Utility may determine appropriate to send to individuals impacted or potentially impacted by the Data Security Incident; and (3) and/or the provision of any credit reporting service required by law or that Utility deems appropriate to provide to such individuals. In addition, within thirty (30) days of confirmation of a Data Security Incident, ESE shall develop and execute a plan, subject to Utility's approval, which approval will not be unreasonably withheld, that reduces the likelihood of a recurrence of such Data Security Incident. ESE agrees that Utility may at its discretion and without penalty immediately suspend performance hereunder and/or terminate the Agreement if a Data Security Incident occurs and it has a reasonable belief of potential ongoing harm. Any suspension made by Utility pursuant to this paragraph 11 will be temporary, lasting until the Data Security Incident has ended, the ESE security has been restored to the reasonable satisfaction of the Utility so that Utility IT systems and Confidential Utility Information are safe and the ESE is capable of maintaining adequate security once electronic communication resumes. Actions made pursuant to this paragraph, including a suspension will be made, or subject to dispute resolution and appeal as applicable, pursuant to the UBP or UBP DERS processes as approved by the Commission.

12. Cybersecurity Insurance Required. Commencing by December 1, 2018, ESE shall carry and maintain Cybersecurity insurance in an amount of no less than $5,000,000 per incident. Utility will maintain at least $5,000,000 of Cybersecurity insurance.

13. No Intellectual Property Rights Granted. Nothing in this Agreement shall be construed as granting or conferring any rights, by license, or otherwise, expressly, implicitly, or otherwise, under any patents, copyrights, trade secrets, or other intellectual property rights of Utility, and ESE shall acquire no ownership interest in the Confidential Utility Information. No rights or obligations other than those expressly stated herein shall be implied from this Agreement.

14. Additional Obligations.

a. ESE shall not create or maintain data which are derivative of Confidential Utility Information except for the purpose of performing its obligations under this Agreement or as authorized by the UBP or UBP DERS. For purposes of this Agreement, the following shall not be considered Confidential Utility Information or a derivative thereof: (i) any customer contracts, customer invoices, or any other documents created by ESE that reference estimated or actual measured customer usage information, which ESE needs to maintain for any tax, financial reporting or other legitimate business purposes consistent with the UBP or UBP DERS; and (ii) Data collected by ESE from customers through its website or other interactions based on those customers' interest in receiving information from or otherwise engaging with ESE or its partners.

b. ESE shall comply with all applicable privacy and security laws to which it is subject, including without limitation all applicable Data Protection Requirements and not, by act or omission, place Utility in violation of any privacy or security law known by ESE to be applicable to Utility.

c. ESE shall have in place appropriate and reasonable processes and systems, including an Information Security Program, defined as having completed an accepted Attestation as reasonably determined by the Utility in its discretion, to protect the security of Confidential Utility Information and prevent a Data Security Incident, including, without limitation, a breach resulting from or arising out of ESE's internal use, processing, or other transmission of Confidential Utility Information, whether between or among ESE's Third-Party Representatives, subsidiaries and affiliates or any other person or entity acting on behalf of ESE, including without limitation Third-Party Representatives. The Utility's determination is subject to the dispute resolution process under the UBP or UBP DERS.

d. ESE and Utility shall safely secure or encrypt during storage and encrypt during transmission all Confidential Information.

e. ESE shall establish policies and procedures to provide reasonable and prompt assistance to Utility in responding to any and all requests, complaints, or other communications received from any individual who is or may be the subject of a Data Security Incident involving Confidential Utility Information Processed by ESE to the extent such request, complaint or other communication relates to ESE's Processing of such individual's Confidential Utility Information.

f. ESE shall establish policies and procedures to provide all reasonable and prompt assistance to Utility in responding to any and all requests, complaints, or other communications received from any individual, government, government agency, regulatory authority, or other entity that is or may have an interest in the Confidential Utility Information, data theft, or other unauthorized release of Confidential Utility Information, disclosure of Confidential Utility Information, or misuse of Confidential Utility Information to the extent such request, complaint or other communication relates to ESE's accessing or Processing of such Confidential Utility Information.

g. ESE will not process Confidential Utility Information outside of the United States or Canada absent a written agreement with Utility. For the avoidance of doubt, Confidential Utility Information stored in the United States or Canada, or other countries as agreed upon in writing will be maintained in a secure fashion at a secure location pursuant to the terms and conditions of this Agreement.

15. Specific Performance. The Parties acknowledge that disclosure or misuse of Confidential Utility Information in violation of this Agreement may result in irreparable harm to Utility, the amount of which may be difficult to ascertain and which may not be adequately compensated by monetary damages, and that therefore Utility shall be entitled to specific performance and/or injunctive relief to

enforce compliance with the provisions of this Agreement. Utility's right to such relief shall be in addition to and not to the exclusion of any remedies otherwise available under this Agreement, at law or in equity, including monetary damages, the right to terminate this Agreement for breach and the right to suspend in accordance with the UBP and UBP DERS the provision or Processing of Confidential Utility Information hereunder. ESE agrees to waive any requirement for the securing or posting of any bond or other security in connection with Utility obtaining any such injunctive or other equitable relief.

16. Indemnification. To the fullest extent permitted by law, ESE shall indemnify and hold Utility, its affiliates, and their respective officers, directors, trustees, shareholders, employees, and agents, harmless from and against any and all loss, cost, damage, or expense of every kind and nature (including, without limitation, penalties imposed by the Commission or other regulatory authority or under any Data Protection Requirements, court costs, expenses, and reasonable attorneys' fees) arising out of, relating to, or resulting from, in whole or in part, the breach or non-compliance with this Agreement by ESE or any of its Third-Party Representatives except to the extent that the loss, cost, damage or expense is caused by the negligence, gross negligence or willful misconduct of Utility.

17. Notices. With the exception of notices or correspondence relating to potential or pending disclosure under legal compulsion, all notices and other correspondence hereunder shall be sent by first class mail, by personal delivery, or by a nationally recognized courier service. Notices or correspondences relating to potential or pending disclosure under legal compulsion shall be sent by means of Express Mail through the U.S. Postal Service or other nationally recognized courier service which provides for scheduled delivery no later than the business day following the transmittal of the notice or correspondence and which provides for confirmation of delivery. All notices and correspondence shall be in writing and addressed as follows:

If to ESE, to:

ESE Name:
Name of Contact:
Address:
Phone:
Email:

If to Utility, to:

Utility Name:
Name of Contact:
Address:
Phone:
Email:

A Party may change the address or addressee for notices and other correspondence to it hereunder by notifying the other Party by written notice given pursuant hereto.

18. **Term and Termination.** This Agreement shall be effective as of the date first set forth above and shall remain in effect until terminated in accordance with the provisions of the service agreement, if any, between the Parties or the UBP or UBP DERS and upon not less than thirty (30) days' prior written notice specifying the effective date of termination, provided, however, that any expiration or termination shall not affect the respective obligations or rights of the Parties arising under this Agreement prior to the effective date of termination. Utility may terminate this Agreement if the ESE is decertified under the UBP or DER UBP, has not served customers for two (2) years, or has not had electronic communication, other than by email, with Utility for one (1) year. Further, Utility may terminate this Agreement immediately upon notice to ESE in the event of a material breach hereof by ESE or its Third-Party Representatives. For the purpose of clarity, a breach of Sections 3-4, 6-11, 13, 14, 16, and 24 shall be a material breach hereof. Upon the expiration or termination hereof, neither ESE nor its Third-Party Representatives shall have any further right to Process Confidential Utility Information or Customer Information and shall immediately comply with its obligations under Section 8 and the Utility shall not have the right to process Confidential ESE Information and shall immediately comply with its obligations under Section 8.

19. **Consent to Jurisdiction; Selection of Forum**. ESE irrevocably submits to the jurisdiction of the Commission and courts located within the State of New York with regard to any dispute or controversy arising out of or relating to this Agreement. ESE agrees that service of process on it in relation to such jurisdiction may be made by certified or registered mail addressed to ESE at the address for ESE pursuant to Section 11 hereof and that such service shall be deemed sufficient even under circumstances where, apart from this Section, there would be no jurisdictional basis for such service. ESE agrees that service of process on it may also be made in any manner permitted by law. ESE consents to the selection of the New York State and United States courts within _____ County, New York as the exclusive forums for any legal or equitable action or proceeding arising out of or relating to this Agreement. If the event involves all of the Utilities jurisdiction will be in Albany County, New York.

20. **Governing Law.** This Agreement shall be interpreted and the rights and obligations of the Parties determined in accordance with the laws of the State of New York, without recourse to such state's choice of law rules.

21. **Survival.** The obligations of ESE under this Agreement shall continue for so long as ESE and/or ESE's Third-Party Representatives continue to have access to, are in possession of or acquire Confidential Utility Information even if all Agreements between ESE and Utility have expired or been terminated.

22. **Counterparts.** This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which shall together constitute

one and the same instrument. Copies of this Agreement and copies of signatures on this Agreement, including any such copies delivered electronically as a .pdf file, shall be treated for all purposes as originals.

23. Amendments; Waivers. Except as directed by the Commission, this Agreement may not be amended or modified except if set forth in writing signed by the Party against whom enforcement is sought to be effective. No forbearance by any Party to require performance of any provisions of this Agreement shall constitute or be deemed a waiver of such provision or the right thereafter to enforce it. Any waiver shall be effective only if in writing and signed by an authorized representative of the Party making such waiver and only with respect to the particular event to which it specifically refers.

24. Assignment. This Agreement (and the Utility's or ESE's obligations hereunder) may not be assigned by Utility, ESE or Third Party Representatives without the prior written consent of the non-assigning Party, and any purported assignment without such consent shall be void. Consent will not be unreasonably withheld.

25. Severability. Any provision of this Agreement which is determined by any court or regulatory body having jurisdiction over this Agreement to be invalid or unenforceable will be ineffective to the extent of such determination without invalidating the remaining provisions of this Agreement or affecting the validity or enforceability of such remaining provisions.

26. Entire Agreement. This Agreement (including any Exhibits hereto) constitutes the entire Agreement between the Parties with respect to the subject matter hereof and any prior or contemporaneous oral or written Agreements or understandings with respect to such subject matter are merged herein. This Agreement may not be amended without the written Agreement of the Parties.

27. No Third-Party Beneficiaries. This Agreement is solely for the benefit of, and shall be binding solely upon, the Parties and their respective agents, successors, and permitted assigns. This Agreement is not intended to benefit and shall not be for the benefit of any party other than the Parties and the indemnified parties named herein, and no other party shall have any right, claim, or action as a result of this Agreement.

28. Force Majeure. No Party shall be liable for any failure to perform its obligations in connection with this Agreement, where such failure results from any act of God or governmental action or order or other cause beyond such Party's reasonable control (including, without limitation, any mechanical, electronic, or communications failure) which prevents such Party from performing under this Agreement and which such Party is unable to prevent or overcome after the exercise of reasonable diligence. For the avoidance of doubt a Data Security Incident is not a force majeure event.

29. Relationship of the Parties. Utility and ESE expressly agree they are acting as independent contractors and under no circumstances shall any of the employees

of one Party be deemed the employees of the other for any purpose. Except as expressly authorized herein, this Agreement shall not be construed as authority for either Party to act for the other Party in any agency or other capacity, or to make commitments of any kind for the account of or on behalf of the other.

30. Construction. This Agreement shall be construed as to its fair meaning and not strictly for or against any party.

31. Binding Effect. No portion of this Agreement is binding upon a Party until it is executed on behalf of that Party in the space provided below and delivered to the other Party. Prior to such execution and delivery, neither the submission, exchange, return, discussion, nor the negotiation of this document, whether or not this document is then designated as a "draft" document, shall have any binding effect on a Party.

[signature page follows]

IN WITNESS WHEREOF, the Parties have executed and delivered this Agreement as of the date first above written.

UTILITY	**ESE**
By: _____	By: _____
Name: _____	Name: _____
Title: _____	Title: _____

SELF-ATTESTATION
OF INFORMATION SECURITY CONTROLS

Each Utility, for itself only, represents that for all information received from Third Party in response or pursuant to this Self-Attestation that is marked CONFIDENTIAL by Third Party (Confidential Self-Attestation Information) Utility shall: (A) hold such Confidential Self-Attestation Information in strict confidence; (B) not disclose such Confidential Self-Attestation Information to any other person or entity; (C) not Process such Confidential Self-Attestation Information outside of the United States or Canada; (D) not Process such Confidential Self-Attestation Information for any purpose other than to assess the adequate security of Third party pursuant to this Self-Attestation and to work with Third party to permit it to achieve adequate security if it has not already done so; (E) limit reproduction of such Confidential Self-Attestation Information; (F) store such Confidential Self-Attestation Information in a secure fashion at a secure location in the United States or Canada that is not accessible to any person or entity not authorized to receive such Confidential Self-Attestation Information under the provisions hereof; (G) otherwise use at least the same degree of care to avoid publication or dissemination of such Confidential Self-Attestation Information as Utility employs (or would employ) with respect to its own confidential information that it does not (or would not) desire to have published or disseminated, but in no event less than reasonable care.

The Requirements to complete the Self-Attestation are as follows (check all that apply to Third Party's computing environment, leave blank all that do not apply to Third Party's computing environment. For items that do not apply. If there are plans to address items that do not currently apply within the next 12 months, place an asterisk in the blank and the month/year the requirement is projected to apply to the Third Party's computing environment), comments regarding plans for compliance are encouraged:

This SELF-ATTESTATION OF INFORMATION SECURITY CONTROLS ("Attestation"), is made as of this _____ day of _____, 20___ by _____, a third party ("Third Party") to Consolidated Edison Company of New York, Inc., Orange and Rockland Utilities, Inc., Central Hudson Gas & Electric Corporation, National Fuel Gas Distribution Corporation, The Brooklyn Union Gas Company d/b/a National Grid NY, KeySpan Gas East Corporation d/b/a National Grid, and Niagara Mohawk Power Corporation d/b/a National Grid, New York State Electric & Gas Corporation and Rochester Gas and Electric Corporation (together, the New York State Joint Utilities or "JU").

WHEREAS, Third Party desires to retain access to certain Confidential Utility Information[1] (as defined in this Data Security Agreement), Third Party must THEREFORE self-attest to Third Party's compliance with the Information Security Control Requirements ("Requirements") as listed herein. Third Party acknowledges that non-compliance with any of the Requirements may result in the termination of utility data access as per the discretion of any of the JU, individually as a Utility or collectively, in whole or part, for its or their system(s). Any termination process will proceed pursuant to the Uniform Business Practices or Distributed Energy Resources Uniform Business Practices.

_____ An Information Security Policy is implemented across the Third Party corporation which includes officer level approval.

_____ An Incident Response Procedure is implemented that includes notification within 48 hours of knowledge of a potential incident alerting utilities when Confidential Utility Information is potentially exposed, or of any other potential security breach.

_____ Role-based access controls are used to restrict system access to authorized users and limited on a need-to-know basis.

_____ Multi-factor authentication is used for all remote administrative access, including, but not limited to, access to production environments.

_____ All production systems are properly maintained and updated to include security patches on a periodic basis. Where a critical alert is raised, time is of the essence, and patches will be applied as soon as practicable.

_____ Antivirus software is installed on all servers and workstations and is maintained with up-to-date signatures.

_____ All Confidential Utility Information is encrypted in transit utilizing industry best practice encryption methods.

_____ All Confidential Utility Information is secured or encrypted at rest utilizing industry best practice encryption methods, or is otherwise physically secured.

[1] "Confidential Utility Information" means, collectively, aggregated and customer -specific information that Utility is: (A) required by the Uniform Business Practices ("UBP") at Section 4: Customer information(C)(2), (3) or Distributed Energy Provider ("DER") UBP at Section 2C: Customer data, to provide to ESCO, Direct Customer or DER Supplier and or (B) any other Data provided to ESE by Utility and marked confidential by the Utility at the time of disclosure, or (C) a Utility's operations and/or systems, including but not limited to log-in credentials, but excludes (i) information which is or becomes generally available to the public other than as a result of a disclosure by Receiving Party or its Representatives; (ii) information which was already known to Receiving Party on a non-confidential basis prior to being furnished to Receiving Party by Disclosing Party; (iii) information which becomes available to Receiving Party on a non-confidential basis from a source other than Disclosing Party or a representative of Disclosing Party if such source was not subject to any prohibition against transmitting the information to Receiving Party and was not bound by a confidentiality agreement with Disclosing Party; (iv) information which was independently developed by the Receiving Party or its Representatives without reference to, or consideration of, the Confidential Information; or (v) information provided by the customer with customer consent where the customer expressly agrees that the information is public.

_____ It is prohibited to store Confidential Utility Information on any mobile forms of storage media, including, but not limited to, laptop PCs, mobile phones, portable backup storage media, and external hard drives, unless the storage media or data is encrypted.

_____ All Confidential Utility Information is stored in the United States or Canada only, including, but not limited to, cloud storage environments and data management services.

_____ Third Party monitors and alerts their network for anomalous cyber activity on a 24/7 basis.

_____ Security awareness training is provided to all personnel with access to Confidential Utility Information.

_____ Employee background screening occurs prior to the granting of access to Confidential Utility Information.

_____ Replication of Confidential Utility Information to non-company assets, systems, or locations is prohibited.

_____ Access to Confidential Utility Information is revoked when no longer required, or if employees separate from the Third Party.

Additionally, the attestation of the following item is requested, but is NOT part of the Requirements:

_____ Third Party maintains an up-to-date SOC II Type 2 Audit Report, or other security controls audit report.

IN WITNESS WHEREOF, Third Party has delivered accurate information for this Attestation as of the date first above written.

Signature: _____

Name: _____

Title: _____

Date: _____

THIRD-PARTY REPRESENTATIVE AGREEMENT

This Third-Party Agreement to be provided to the Utility upon request.

I, _____, have read the Agreement between _____, ("Company") and _____, ("Utility") dated _____ __, 20__ (the "Agreement") and agree to the terms and conditions contained therein. My duties and responsibilities on behalf of _____ require me to have access to the Confidential Information disclosed by Utility to the ESE pursuant to the Agreement.

_____ _____

Signature Date

Mary Krayeske
Associate Counsel
Law Department

November 9, 2018

Honorable Kathleen Burgess
Secretary
State of New York Public Service Commission
Three Empire State Plaza
Albany, NY 12223-1350

Re: **Case 98-M-1343 – In the Matter of Retail Access Business Rules**
Case 18-M-0376 -- Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place

Dear Secretary Burgess:

Attached is a *Petition of the Joint Utilities for Declaratory Ruling Regarding their Authority to Discontinue Utility Access to Energy Service Companies in Violation of the Uniform Business Practice*s on behalf of Central Hudson Gas & Electric Corporation, Consolidated Edison Company of New York, Inc., National Fuel Gas Distribution Corporation, New York State Electric and Gas Corporation, The Brooklyn Union Gas Company d/b/a National Grid, Niagara Mohawk Power Corporation d/b/a National Grid, Orange and Rockland Utilities, Inc., and Rochester Gas and Electric Corporation

If there are any questions, please contact me.

Sincerely,

/s/ *Mary Krayeske*

Mary Krayeske

Attachment

STATE OF NEW YORK
PUBLIC SERVICE COMMISSION

In the Matter of Retail Access Business Rules	**Case 98-M-1343**
Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place	**Case 18-M-0376**

PETITION OF THE JOINT UTILITIES FOR DECLARATORY RULING REGARDING THEIR AUTHORITY TO DISCONTINUE UTILITY ACCESS TO ENERGY SERVICE COMPANIES IN VIOLATION OF THE UNIFORM BUSINESS PRACTICES

Pursuant to 16 N.Y.C.R.R. Part 8 and the Uniform Retail Access Business Practices ("UBP"),[1] Consolidated Edison Company of New York, Inc., Orange and Rockland Utilities, Inc., Central Hudson Gas & Electric Corporation, National Fuel Gas Distribution Corporation, The Brooklyn Union Gas Company d/b/a National Grid NY, KeySpan Gas East Corporation d/b/a National Grid, and Niagara Mohawk Power Corporation d/b/a National Grid, New York State Electric & Gas Corporation and Rochester Gas and Electric Corporation ("Petitioners" or "Joint Utilities") petition the Public Service Commission (the "Commission") to issue a declaratory ruling confirming the Joint Utilities' right under the UBP to discontinue an Energy Service Company's ("ESCO") access to Petitioners' various systems, in their relevant retail access program, if that ESCO fails to meet minimum data

[1] Revised February 2016, pursuant to Case 98-M-1343, In the Matter of Retail Access Business Rules. *Order Authorizing Accelerated Switching of Natural Gas Commodity Suppliers and Related Matters* (issued December 23, 2015).

security standards, including the execution of a Data Security Agreement ("DSA") in accordance with UBP provisions governing "Eligibility Requirements" for ESCOs.[2]

I. BACKGROUND

Pursuant to 16 NYCRR § 8.1(a),[3] the Joint Utilities request a declaratory ruling confirming that each utility can discontinue an ESCO's participation in its retail access program for failure to meet minimum data security standards pursuant to the Commission's UBP requirements for ESCOs. The specific UBP rule the Joint Utilities would enforce states that they can discontinue an ESCO's participation in a retail access program for the following reason:

> Failure to act that is likely to cause, or has caused, a significant risk or condition that compromises the safety, *system security*, or operational reliability of the distribution utility's system, and the ESCO or Direct Customer failed to eliminate immediately the risk or condition upon verified receipt of a non-EDI notice.[4] *[emphasis added]*

An ESCO's refusal or failure to meet minimum data security requirements, including a refusal to execute the DSA, poses a significant risk that compromises utility and ESCO system security and the privacy of customer data. An ESCO's failure or refusal in this regard justifies discontinuance from access to utilities' various systems.

Cyber and data security are critical concerns for the Commission, customers, stakeholders, and the Joint Utilities. As the Commission stated in its June 14, 2018 *Order*

---

[2] UBP Section 2.
[3] 16 N.Y.C.R.R. Sec. 8.1(a) provides that the Commission may issue a declaratory ruling as to the applicability to any person, property, or state of facts or any rule or statute enforceable by the Commission or the validity of such a rule or whether the Commission should take action pursuant to a rule.
[4] UBP at 11-12 (Section 2: Eligibility Requirements (F).1.a).

Instituting Proceeding, in Case 18-M-0376 (the "Order"), "Cyber security threats have become a common occurrence, and the industry must be vigilant in order to protect against, detect, and respond to these events."[5] The Commission further stated that "a recent cyber event impacting the energy services market makes clear that additional attention is needed to ensure that appropriate protections are being implemented and followed throughout the industry."[6] Finally, as the Commission recognized in the Order, the Joint Utilities, Department of Public Service Staff ("Staff"), ESCOs and energy service entities ("ESEs") "agree with the need for adequate cyber security protections."[7] ESEs also maintain customer data and connect with utility systems to acquire utility and customer data when authorized to do so by the customer.

Pursuant to the Order, the Joint Utilities have been collaborating with Staff, ESCOs, and other ESEs, which include electronic data interchange ("EDI") providers and direct customers, to determine the appropriate roles and responsibilities for protecting customer data and systems and infrastructure from cyber incidents.[8] The Joint Utilities take this obligation seriously and work with contractors and vendors to address ongoing security efforts.

As outlined in the Order, Staff, the Joint Utilities, ESCOs, ESEs, and other stakeholders have continued the established collaborative business-to-business process to develop a uniform DSA and accompanying Self Attestation form. The business-to-

---

[5] Case 18-M-0376, Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place ("Cyber Security Proceeding"), *Order Instituting Proceeding* (issued June 14, 2018), at p. 2.
[6] *Id.*
[7] *Id.*
[8] See, New York Public Service Law, Section 65.1.

business process included numerous opportunities for stakeholder participation over several months, including two rounds of written comments, three days of in-person technical conferences,[9] and multiple teleconferences.[10]

The DSA that resulted from that effort includes a Self-Attestation form to be completed by the ESCOs and ESEs attesting to the technical cyber security protocols in place and maintained by the ESCOs and ESEs. The DSA, with the accompanying Self Attestation, establishes a minimum cyber security standard for utilities, ESCOs, and ESEs participating in New York energy markets to protect their respective systems and customer data. Importantly, the DSA imposes mutual obligations upon the Joint Utilities, ESCOs, and ESEs to protect confidential utility, ESCO, ESE, and customer data. Upon finalizing the forms, each of the Joint Utilities circulated the DSA and Self Attestation to all ESCOs and ESEs for review and execution and requested return of these documents by August 31 and August 18, respectively.[11]

In addition, as required by the Order, at the end of the business-to-business process, Staff filed its *Report on the Status of the Business-to-Business Collaborative to Address Cyber Security in the Retail Access Industry* (the "Staff Report").[12] As Staff noted therein, the end result of the business-to-business process was a DSA that varied from the Joint Utilities original proposed version, and "strikes a fair balance between the Joint Utilities'

---

[9] May 31, 2018, and July 26-27, 2018.
[10] In addition, a working group site on the Department of Public Service web page was established to maintain all documents related to the Cyber Security Proceeding. The URL for the web page is: http://www3.dps.ny.gov/W/PSCWeb.nsf/All/4A24D0D51395B1F8852582A2004398A3?OpenDocument.
[11] Going forward, the Joint Utilities will require new ESCOs and ESEs to provide a DSA and Self-Attestation prior to performing EDI testing.
[12] Case 18-M-0376, *Department of Public Service Staff Report on the Status of the Business-to-Business Collaborative to Address Cyber Security in the Retail Access Industry* (issued September 24, 2018).

concerns of both protecting the utility systems from infiltration and against customer data breaches, and the ESE's concerns of overreaching and over-burdensome cyber security requirements."[13] Further, Staff observed that the "Self-Attestation consists of a 16-point inventory of cyber controls based on National Institute of Standards and Technology ("NIST") standards, and requested that ESCOs and ESEs attest that they observe these minimum standards, or if the ESE is not already doing so, to implement these controls within a reasonable timeframe."[14]

Most ESCOs and ESEs executed DSAs and Self Attestations, committing to take the necessary steps to implement appropriate protections of customer data and ESCO, ESE, and associated systems. Currently, the Joint Utilities have received signed DSAs and Self Attestations that provide cyber protections for approximately 90 percent of customers participating in the New York energy markets.

Nevertheless, there remains a small group of ESCOs (the "Non-participating ESCOs") that have either failed or refused to sign the DSA or complete the Self - Attestation, or both. In addition, some Non-participating ESCOs failed to engage in the business-to-business process and some now seek to delay the process or reject the business-to-business process entirely. Some seek further technical discussions to discuss further modifications to the current DSA and Self Attestation.[15] To the extent the Non-participating ESCOs state that widely accepted cyber security protections/defenses are not

---

[13] *Id*. at 4-5.
[14] Staff Report p. 4.
[15] Some Non-participating ESCOs have submitted comments formally in the Cyber Security Proceeding, summarizing their various positions.

necessary or justified, these positions were either incorporated, rejected or folded into the larger compromise to achieve the current DSA terms.

Notwithstanding the robust negotiation process, reasonable compromise positions reached by both Joint Utilities and ESEs, and ultimate execution by the vast majority of ESCOs, the Non-participating ESCOs have foregone execution of the DSA and completion of the Self Attestation. This petition follows a sound process that considered all stakeholders' concerns collaboratively, recognizing the urgency and importance of establishing minimum requirements for data security and the need to provide an opportunity for all interested stakeholders to provide input into the process.

II. Need for Declaratory Ruling

A small number of Non-participating ESCOs have failed to commit to adequate data security to meet the minimum cyber security standards required to participate in the retail access program as required by the Commission. Accordingly, the Joint Utilities request that the Commission affirm the Joint Utilities' right to discontinue these Non-Participating ESCOs' ability to participate in the relevant retail choice programs and to deny access to the Joint Utilities' systems and data.

Without executed DSAs and Self Attestations, the Joint Utilities and their customers are exposed to cyber security risks, including data and financial risk. These risks include the ability of the ESCO or ESE to harm a utility system during the regular exchange of information as well as the potential loss of customer data. The Joint Utilities have controls in place intended to reduce the risk that the information exchange could cause a cyber security issue, yet there remains a risk. For their part, the ESCOs and the ESEs need to have controls in place to assure the Joint Utilities that they are safeguarding

customer information, because a loss of this type of information could be significant and include the potential for customer identity theft.

The Staff Report addressed each of the concerns raised by the Non-participating ESCOs and concluded that, those concerns notwithstanding, moving forward promptly with signed DSAs and Self Attestations is warranted. Delaying efforts to close this gap in cyber protections only prolongs the period that utilities and their customers are unprotected.

Given the risks, the Joint Utilities must be able to protect the security and operation of utility systems if ESCOs and ESEs do not provide the DSAs and/or Self Attestations. Under Section F of the UBP, the Joint Utilities have the right to discontinue service to Non-participating ESCOs that fail to comply with UBP eligibility requirements, including a Non-participating ESCO's failure to provide a signed DSA and completed Self Attestation to meet minimum cyber security standards and maintain the security and operational reliability of utility systems. Permitting Non-participating ESCOs to maintain access to utility customer systems while circumventing or avoiding minimum cyber security standards poses an unreasonable risk to utility systems and perpetuates a gap in data security. The Joint Utilities' and customers' interest in having adequate data security is of paramount interest to all stakeholders. As shown above, the UBP specifically permits a utility to discontinue an ESCO's participation in the retail access program where there is significant risk that compromises the safety, system security, or operational reliability of the distribution utility's systems.[16]

[16] UBP Section 2(F).

The Joint Utilities believe the UBPs permit individual utilities to initiate the discontinuance process pursuant to UBP Section 2(F)(2) without intervention of the Commission. However, the Joint Utilities request that the Commission confirm the Joint Utilities' right under the UBP to discontinue certain ESCOs access to Petitioners' various systems and retail access program, if that ESCO fails to meet minimum data security standards.[17]

III. CONCLUSION

Granting the requested relief is necessary to maintain minimum cyber security standards established by the stakeholders pursuant to the business-to-business process adopted by the Commission in this proceeding and is necessary to fully protect the interests of customer data privacy and utility cyber security. For these reasons, Petitioners respectfully urge the Commission to issue a declaratory ruling affirming the Joint Utilities' right under the UBP to discontinue certain ESCOs access to Petitioners' various systems and retail access program, if that ESCO fails to meet minimum data security standards in accordance with the UBP, including executing and complying with the DSA. Given the importance of maintaining proper cyber security protocols, the Joint Utilities urge the Commission to act expeditiously in making this declaration.

Paul A. Colbert Associate General Counsel- Regulatory Affairs Central Hudson Gas & Electric Corporation 284 South Avenue Poughkeepsie, NY 12601 pcolbert@cenhud.com	Justin Atkins Counsel, Avangrid Networks Corporate Secretary, CMP and MEPCO New York State Electric & Gas Corporation and Rochester Gas and Electric Corporation 89 East Avenue Rochester, New York 14604

[17] After the issuance of the declaratory ruling, the Joint Utilities would notify the ESCOs and ESEs who remain in non-compliance.

	Justin.atkins@avangrid.com
Mary Krayeske Associate Counsel Kerri Kirschbaum Associate Counsel Consolidated Edison Company of New York, Inc. and Orange and Rockland Utilities, Inc. 4 Irving Place New York, NY 10003-0987 Krayeskem@coned.com kirschbaumk@coned.com	Michael E. Novak Assistant General Manager Ty A. Holt, Esq. Senior Attorney Rates & Regulatory Affairs 6363 Main Street Williamsville, NY 14221 novakm@natfuel.com holtt1@natfuel.com
Jeremy J. Euto Senior Counsel II National Grid 300 Erie Blvd West Syracuse, NY 13202 315-428-3310 jeremy.euto@nationalgrid.com	

DERS' Summarized Written Comments

The comments are noted and numbered, then followed by the Joint Utilities reply immediately below the comment. In some cases, the response goes to more than one argument.

(1) Confidential customer information must be protected and cyber security protection must be in place when a utility transfers information to an ESE;[1]

(2) UBP DERS Section 2(C) does not apply to DERS;[2]

(3) If the DSA and similar cyber security regulations are applied to DERS the DERS may not provide value added services and the DERS market may not grow;[3]

Comments (1), (2), and (3) are addressed within the Petition itself.

(4) Obtaining customer authorization is adequate protection in lieu of the proposed SA and DSA;[4]

In response to comment 4, customer authorization, is not a substitute for cyber security measures. No customer is authorizing a DERS to allow its data to be used or released through the actions of a cyber-criminal or the negligence of a DERS who allows an inadvertent release of data or malware.

---

[1] Case 18-M-0376 - *Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place* (Comments of Energy Technology Savings, Inc. DBA Logical Buildings (hereinafter "Logical Buildings") at 2) (December 13, 2018); AEMA Comments at 4 (December 14, 2018); CPA Comments at 2-4) (December 14, 2018); Blueprint Comments at 1) (December 21, 2018).
[2] *Id*. (Comments of Logical Buildings at 2) (December 13, 2018); CPA Comments at 2-3) (December 14, 2018); (AES Comments at 2) (December 14, 2018).
[3] *Id*. (Comments of Logical Buildings at 2) (December 13, 2018); CPA Comments at 2-3) (December 14, 2018).
[4] *Id*. (Comments of Logical Buildings at 2) (December 13, 2018); (CPA Comments at 6) (December 14, 2018); (AES Comments at 2) (December 14, 2018).

(5) Instead of the SA and DSA, the Commission could require DERS to have a non-disclosure agreement ("NDA") with third parties with which they share confidential customer data necessary for the DERS to provide services to customers;[5]

Regarding comment 5, an NDA with a Third Party Representative is not a substitute for adequate cyber security measures implemented and maintained by the DERS and the Third Party Representative unless the NDA requires cyber security terms and conditions at least as stringent as those in the SA and DSA.

(6) DSA requirements should be applied to EDI providers but not to other entities with whom DERS may contract;[6]

Comment 6 suggests that no ESE or Third Party Representative, other than an EDI provider, need comply with the DSA. Unfortunately, if the DERS contracts with other parties that have access to the Confidential Information and have electronic transactions with the DERS or utility, other than by email, risks to the Confidential Information and IT systems of the DERS and utility remain. It is standard contract language that a counter-party to a contract is responsible for the conduct of subcontractors and must require their subcontractors to abide by the terms and conditions of the contract.

(7) DERS should not be liable for the actions of their Third Party Representatives;[7]

Comment 7 is similar to comment 6 in that DERS are trying to avoid liability for their subcontractors. Liability could not be avoided in a normal contract for goods or

[5] *Id*. (Comments of Logical Buildings at 3) (December 13, 2018); (CPA Comments at 6) (December 14, 2018).
[6] *Id*. (Comments of Logical Buildings at 2) (December 13, 2018); (CPA Comments at 5) (December 14, 2018).
[7] *Id*. (Comments of Logical Buildings at 2) (December 13, 2018); (DSA Coalition Comments at 2-4) (December 14, 2018); (CPA Comments at 5) (December 14, 2018).

services nor should it be permitted regarding the DSA where a cyber security incident may cause significant physical, reputational, and financial damage to customers and the utility by releasing or changing Confidential Information and harming IT systems.

(8) The Joint Utilities should clarify whether the definition of contractor is the same as the definition of Third Party Representative in the DSA;[8]

Comment 8 asks whether the definition of contractor is the same as the definition of Third Party Representative in the DSA. There is no definition of "contractor" in the DSA. A Third Party Representative is defined as:

> [T]hose agents acting on behalf of ESCOs, Direct Customers, or DERS that are contractors or subcontractors and that store, transmit or process Confidential Utility Information. For the avoidance of doubt, Third-Party Representatives do not include ESEs and their members, directors, officers or employees who need to know Confidential Utility Information for the purposes of providing Services.[9]

Third Party Representatives must be contractors of the ESCO, DERS, or Direct Customers. The language is clear and no amendment or clarification to the DSA is needed.

(9) The DSA should apply only to DERS that transact directly with the utility and only to information obtained from the utility;[10]

Comment 9 would limit the applicability of the DSA to DERS that transact directly with the utility and only to information received by the DERS from the utility. It is undisputed that DERS, like ESCOs and Direct Customers, may use Third Party Representatives to perform a variety of services, including the direct electronic

[8] *Id*. (Comments of Logical Buildings at 4) (December 13, 2018).
[9] DSA at 3-4.
[10] *Id*.

transmission of Confidential ESE Information to the utility and the receipt of Confidential Utility Information from the utility.

Third Party Representatives may also receive and process Confidential ESE and Utility Information at the direction of the DERS, ESCO, or Direct Customer. In each instance, the DERS must require compliance by the Third Party Representative with the DSA because it is in privity—has a contract with—the Third Party Representative, while the utility is not. The utility cannot compel the Third Party Representative to implement and maintain cyber security or submit the DSA, only the DERS, ESCO, or Direct Customer may so compel.

Also, if the DERS ESCO, or Direct Customer fails to require their Third Party Representative to comply with the DSA, they must be liable for the failure whether they are directly electronically transacting with the utility or not. Similarly, only the DERS, ESCO, and Direct Customer receive customer authorization and collect Confidential ESE Information from the customer and maintain it and/or provide it to the utility. They are limited in what they are permitted to do with the customer data that is part of the Confidential ESE Information. The DSA should apply to the Confidential Utility Information and the Confidential ESE Information.

(10) The DSA should apply only to Third Party Representatives that transact directly with the utility;[11]

(11) Audit provisions should not apply to Third Party Representatives that do not directly interact with the utility;[12]

[11] *Id*.
[12] *Id*.

(12) Third Party Representatives should not be required to maintain cyber security insurance unless they directly interact with the utility;[13]

Regarding comments 10 and 11, the DSA should apply to all Third Party Representatives, not just those that transact directly with the utility, for the same reason as set forth in the response to comment 9. The same reasoning that applies to comments 9, 10, and 11 apply to comment 12. The risks associated with Third Party Representatives that receive Confidential Utility Information indirectly are no different than those that receive it directly.

(13) With customer authorization, the DERS must be able to retain customer data and use it as the DERS determines is necessary to serve customers;[14]

Comment 13 is incorrect. The DER UBP at Section 2C(B)(1), 2C(E) require the DERS to disclose to the customer "the types of information to be obtained, to whom it will be given, how it will be used, and how long the authorizations will be valid…" and:

> is prohibited from selling, disclosing or providing any customer information obtained from a distribution utility or DSP, in accordance with this Section, to others, including their affiliates, unless such sale, disclosure or provision is required to facilitate or maintain service to the customer or is specifically authorized by the customer or required by legal authority.

The DSA, at Section 14(a), prohibits the ESE, including DERS, from creating or maintaining data that is derivative of Confidential Utility Data. Regarding Confidential ESE Data, the DSA at Section 3, merely requires the ESE to comply with the UBP and UBP DERS. The UBP DERS permits the DERS to use the data for its own purposes if

[13] *Id*.
[14] *Id*. (Comments of Logical Buildings at 2) (December 13, 2018); (DSA Coalition Comments at 2-4) (December 14, 2018); (CPA Comments at 8) (December 14, 2018).

the customer is informed of and authorizes the use. No amendment is required to the DSA based on comment 13.

(14) Certain entities with sterling reputation that interact with utilities directly should be exempt from DSA requirements including cyber insurance;[15]

Comment 14 suggests that certain entities, such as IBM and Google, be exempted from the DSA requirements even if they are Third Party Representatives. Large experienced entities must adhere to the DSA's requirements. To exempt them would weaken cyber security and would not make them expressly liable for their failure, weakening the DSA's financial protections for customers and utilities. The Joint Utilities, however, recognize that there are times when some counterparties refuse to agree, or even negotiate, but are necessary to the transaction. If such an issue arises, the Joint Utilities encourage the DERS to discuss the issue with the applicable utility to try to resolve the issue, but the DSA should apply consistently to all Third Party Representatives.

(15) Required encryption of confidential information transmitted by email is overly burdensome;

Comment 15 seeks to eliminate encryption. Encryption is a basic cyber security requirement and is not burdensome but is necessary to protect confidential data and IT systems. Encryption is embedded in every cyber security protocol including NIST. Encryption requirements should not be stricken from the DSA.

[15] *Id*. at 5.

(16) The DSA should not apply to DERS that engage only with large commercial and industrial customers;[16]

Through comment 16, the DERS seek an exemption from compliance with the DSA if they serve only large commercial and industrial customers. There is no evidence that a DERS serving large commercial and industrial customers has less cyber security risk than a DERS serving mass market customers. Criminals target the weak link, whether it is the DERS or its customers. The submission of the DSA already represent a minimal level of cyber security. If a large commercial or industrial customer is required to, but cannot, comply with the DSA, then it does not have adequate cyber security and is a cyber security risk. If a large commercial or industrial customer can comply with the DSA cyber security requirements, there is no harm in requiring them to comply. In all instances, the DERS should submit the DSA.

(17) The DSA's indemnification and audit clauses should be amended so that (i) DERS are not strictly liable except for utility negligence, (ii) audits may happen only if there is a cyber security event, and (iii) add a limitation of liability clause so that DERS are not liable for more than one million dollars;[17]

Comment 17 represents another comment where the DERS are simply trying to avoid or shift liability. The indemnification and audit clauses have been the subject of extensive discussion and comment. The indemnification clause has already been the subject of compromise by alleviating ESE liability and that of its Third Party Representatives to the extent that the utility is negligent.[18] The audit clause limits the

[16] Case 18-M-0376 - *Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place* (AEMA Comments at 5) (December 14, 2018).
[17] *Id*. at 6.
[18] DSA at 11.

right of the utility to audit to once annually, which is a standard contract term and condition. Audit rights are necessary to encourage compliance. The suggestion of a limitation of liability clause that limits liability to $1,000,000 is unacceptable because damages may be much more. That is why cyber security insurance is required. The amount of insurance has been lowered from $10,000,000 to $5,000,000 against the advice of the Joint Utilities because even $10,000,000 of cyber security insurance is inadequate to cover the costs of a significant cyber security incident. If the DERS want more protection, rather than limit their liability, they should purchase more insurance. A limitation of liability clause does nothing more than shift financial risk from the DERS to customers and the utility.

(18) The Commission may need to create a dispute resolution process;[19]

Comment 18 suggests that the Commission may need to form a dispute resolution process. The Joint Utilities do not object to the creation of a formal dispute resolution process by the Commission, but such formation does not require an amendment to the DSA. The DSA already states in Sections 11, 14(c), and 19 that disputes are subject to the Commission's jurisdiction.

(19) As a matter of process, the Commission should approve the DSA and SA;[20]

By this Petition, the Joint Utilities ask that the Commission approve the process to formulate the SA and DSA, including continuing workshops to amend them going forward, rather than approve the specific SA and DSA. The Joint Utilities also ask that the Commission approve standard DSA provisions so that these important provisions permanently remain part of the DSA. Process approval allows for the rapid pace of

[19] *Id*.
[20] *Id*. at 7.

change to cyber security requirements, and therefore, necessarily rapid changes to the DSA. However, as for future changes, Waiting for a formal Commission approval through the SAPA process each time a change is needed may raise the cyber security risks or needlessly maintain costly cyber security practices. A nimble process with dispute resolution before the Commission adequately protects all ESEs, Third Party Representatives, customers, and utilities.

(20) Cyber security standards should be applied on an individualized risk basis instead of through standardized agreements;[21]

Comment 20 seeks to require individually negotiated DSAs rather than a standard DSA applicable to all ESEs. That is not a practical solution where the utilities are required to enter electronic transactions with the ESEs. Under the existing regulatory paradigm where the utilities are regulated and required to transact, it is necessary to have a DSA that sets minimum cyber security standards. As it is, if a cyber security event by an ESE occurs, the Joint Utilities must disconnect the ESE to protect utility IT systems and customer information. Each time that happens issues are raised, including but not limited to the speed of notification or lack thereof, whether disconnection is appropriate, responsibility for customer notification and financial liability. The Joint Utilities ask that the Commission affirm their authority to require submission of the DSA by all ESEs combined with a continuing Commission approved process to discuss, refine and amend the DSA as appropriate through ongoing workshops. Such an affirmation by the Commission protects all parties with cyber security responsibility.

[21] Case 18-M-0376 - *Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place* (DSA Coalition Comments at 2-4) (December 14, 2018).

(21) There is an ambiguity in DSA Section 1(d) defining Data Protection Requirements;[22]

Comment 21 raised by DSA Coalition and CPA is confusing. DSA Coalition alleges that DSA Section 1(d) defining Data Protection Requirements conflicts with unspecified language alleging that if an ESE complies with the SA it is in compliance with the DSA and that a DERS is not required to comply with all of the security requirements set forth in the SA to which it attests.[23] Nowhere in the DSA does it say that compliance with the SA is compliance with the DSA or that a DERS that does not have all of the cyber security measures listed in the SA is in compliance with anything or has adequate cyber security. The DSA is a broader document and has more requirements than the SA and a DERS must submit a SA and comply with the DSA. If a DERS submits a SA indicating it lacks some of the cyber security requirements the DERS will be assessed by the applicable utility's IT security personnel and the utility will discuss with the DERS what is necessary over what time frame so that the DERS may achieve adequate cyber security. If the DERS does not achieve adequate cyber security within the timeframe discussed it will be disconnected from the utility IT system or not permitted to connect, whichever is applicable. The SA is a tool for assessment of minimum cyber security, nothing else.

CPA impugns the ability of the Joint Utilities and other ESEs to know, understand, implement, and maintain adequate cyber security, particularly industry best practices and asks that Section 1(d) be deleted.[24] The utilities know what industry best cyber security practices are and have implemented and maintained them. Many ESEs also know what

[22] *Id*. (DSA Coalition Comments at 2-4) (December 14, 2018); (CPA Comments at 7-8) (December 14, 2018).
[23] DSA Coalition Comments at 4-5.
[24] CPA Comments at 7-8.

industry best cyber security practices are and have implemented and maintained them. If an ESE hires a cyber security expert, it is incumbent upon them to keep up with industry best cyber security standards. Contractors that provide cyber security services, often cheaper than employees, also know industry best cyber security standards. Cyber security standards are changing rapidly and becoming more stringent. Section 1(d) is critical to defining the cyber security standards to be maintained and must remain a part of the DSA. Section 1(d) requires no amendment.

(22) DSA Section 5 regarding Provision of Information should state that it is subject to the UBP and UBP DERS;[25]

Comment 22 seeks an explicit statement in DSA Section 5 concerning Provision of Information that it is subject to the procedural processes set forth in the UBP DERS. As the DSA Coalition notes correctly, the DSA already states that it is subject to the UBP and UBP DERS in Sections 1(a), 1(b), 1(d), 1(f), 1(g), 1(h), 1(m), 3, 4, 6, 7(a), 8, 11, 14(a), 14(c), 15, and 18. The reference in DSA Section 3 is a general reference stating that the parties agree that the UBP and UBP DERS govern the protection of Confidential Information and the electronic exchange of information between the Parties. DSA Section 3 provides the assurance that the DSA Coalition seeks. DSA Section 5 lists requirements not covered by the UBP or UBP DERS without disturbing the processes contained in either UBP. Specifically, DSA Section 5 requires the ESE and Third Party Representatives to comply with the DSA, submit the SA and maintain the cyber security set forth in the SA and acceptable to the utility. None of those issues are covered in the UBP or UBP DERS. No amendment to the DSA is required.

[25] *Id*. (DSA Coalition Comments at 5) (December 14, 2018).

(23) Data Security Incident notifications should be agreed to on an incident by incident basis;[26]

Comment 23 requests that Data Security Incident notification requirements be negotiated on a case-by-case basis. DSA Section 11, Data Security Incidents, and the notice provision, in particular, has been the subject of extensive discussion among the Parties. Under at least certain circumstances New York law requires notification "in the most expedient time possible and without unreasonable delay,…"[27] The Joint Utilities have already compromised to allow an ESE to notify the utility of a Data Security Incident within 48 hours. Further delay exponentially increases the risk to customer information and utility IT systems. It is unreasonable to negotiate the notice term on a case-by-case basis or otherwise delay notification. The compromise 48-hour notification requirement set forth in DSA Section 11 should remain unchanged.

(24) Cyber security insurance should be determined on a case-by-case basis;[28]

Comment 24 seeks to negotiate cyber security insurance requirements on a case-by case basis. The $5,000,000 cyber security insurance requirement represents a compromise from the Joint Utilities' original proposal of $10,000,000. Both amounts are less than the expected cost to customers and the utility of a significant cyber security incident. The average cost of a cyber security incident was more than $17 million for financial service, utility and energy companies in 2017.[29] The DSA's cyber insurance requirement should not be changed or negotiated on a case-by-case basis. To protect customers and utility IT systems, it is likely that the required amount of cyber security

[26] *Id*.
[27] General Business Law § 899-aa.
[28] *Id*. at 5-6
[29] 2017 Cost of Cyber Crime Study at 3 (Ponemon Institute LLC).

insurance will increase in the future or the ESE will need to demonstrate an ability to pay the costs associated with a cyber security incident transmitted from its IT system to the utility.

(25) The DSA should permit data to be stored outside the United States and Canada;[30]

Comment 25 asks to permit ESEs to store data governed by the DSA outside of the United States and Canada. As discussed at length during the business-to-business negotiations, the United States Export Administration ("EAR") (15 C.F.R. §§730-774) and the United States International Traffic Arms Regulations ("ITAR") (22 C.F.R. Section (§) 120-130) permit covered information to be stored in the United States and Canada, but not elsewhere. The Joint Utilities have consistently indicated that they will consider requests for storage in other countries if the ESE can demonstrate compliance with EAR and ITAR. No change should be made to the DSA based upon this comment.

(26) The SA should not be effective and binding until the DSA is finalized;[31]

Comment 26 suggests that the SA should not be effective and binding until the DSA is finalized. Most ESEs have submitted SAs. Those ESEs that have not submitted a SA must do so immediately so that minimum standards of cyber security are in place. Absent submission of the ESE, the Joint Utilities cannot make an assessment about whether an ESE has adequate cyber security. The Joint Utilities are committed to working with the ESEs to help them achieve adequate cyber security in a reasonable period of time, but refusal by an ESE to comply with cyber security requirements will ultimately

[30] *Id*. at 6
[31] *Id*.

result in the applicable utility using the UBP or UBP DERS process to disconnect the ESE from the utility's IT system, which may cause an inability to provide service.

(27) Only information designated by the UBP and UBP DERS should be confidential and protected pursuant to the DSA while other information marked confidential by the utility should not be afforded DSA protections;[32]

Comment 27 suggests that the DSA should not apply to Confidential Utility Information other than the information designated as confidential by the UBP and UBP DERS. The mere fact that an ESE is exchanging information electronically, other than by email, with the utility means that there is risk to all information on the utility's IT system because certain types of malware may seek out data that is not the subject of the exchange. Additionally, the ESE may request other types of information from the utility or the utility may need to include certain confidential material in the data exchange that is not the subject of the request. Regardless of the circumstance, the utility has, and maintains the right to mark information as confidential and require the ESE to maintain the confidentiality of the marked material. The ESE has the reciprocal right. The DSA should not be amended based on Comment 27.

(28) Indemnification by DERS should not be required;[33]

Comment 28 asks that DSA Section 16, Indemnification, be stricken because:

> Any major breach could result in tens or hundreds of millions of dollars in costs, costs that no ESE or third party could possibly pay. In addition, the ways in which arguable non-compliance could occur, even unknown to the ESE or third party, are many. Instead, faced with accepting such liability many entities would instead choose to do business elsewhere.[34]

[32] *Id*. (CPA Comments at 5) (December 14, 2018).
[33] *Id*. at 6.
[34] CPA Comments at 6.

It is true that the cost of a cyber security event may be substantial. The average cost in the energy, utility and financial service industry category is over $17,000,000 per incident.[35] If a cyber security incident emanates from an ESE, the ESE must be liable for the damage. Otherwise, liability inappropriately shifts from the ESE to customers or the utility. The solution is for the ESE to maintain adequate cyber security and cyber security insurance, not to eliminate the indemnification provision and shift the liability to customers and/or utilities. Further, some ESEs are large companies, capable of maintaining cost responsibility. The DSA should not be amended based on comment 28.

(29) The DSA should adopt State of New York Office of Information Technology Services standards and one standard, NIST 800-171, instead of a mixture of standards.[36]

Blueprint offered comment 29, which suggests that the DSA should adopt a specific cyber security standard, rather than the cyber security standards listed in DSA Section 1(d), which offers ESEs some flexibility to provide adequate cyber security. Specifically, Blueprint suggests that the standards adopted by the NYITS and/or NIST 800-171 should be adopted.[37] Both sets of standards suggested by Blueprint have been reviewed by the Joint Utilities and are weaker than the cyber security standards contained in DSA Section 1(d).

First, it should be noted that Blueprint refers only to NYITS standard NYS-S14-002, which is but one of many NYITS cyber security standards. Second, NYITS cyber security standard NYS-S14-002 adopts NIST 800-53.[38] That NYITS adopts NIST 800-53

[35] 2017 Cost of Cyber Crime Study at 3 (Ponemon Institute LLC).
[36] *Id*. (Blueprint Comments at 2-3) (December 21, 2018).
[37] Blueprint Comments at 3-4.
[38] NYIST NYS-S14-002 at 6 (https://its.ny.gov/document/information-classification-standard).

is significant because Blueprint asks that instead of NIST 800-53, one of the cyber security protocols permitted by DSA Section 1(d), Blueprint suggests that the DSA use NIST 800-171, which is a lesser standard inappropriate for the cyber security protections necessary to protect customer data and utility IT systems. Blueprint's comments are self-serving because, if adopted, they would lead to weaker cyber security to the detriment of customers and utilities while lowering costs for ESEs and transferring cost liability from ESEs to customers and utilities. Comment (29) should not be adopted and it should not cause an amendment to the DSA.

STATE OF NEW YORK
PUBLIC SERVICE COMMISSION

In the Matter of Regulation and Oversight of Distributed Energy Resource Providers and Products	**Case 15-M-0180**

JOINT UTILITIES' REQUEST FOR CLARIFICATION

Central Hudson Gas & Electric Corporation, Consolidated Edison Company of New York, Inc., New York State Electric & Gas Corporation, Niagara Mohawk Power Corporation d/b/a National Grid, KeySpan Gas East Corporation d/b/a National Grid and The Brooklyn Union Gas Company d/b/a National Grid NY, Orange and Rockland Utilities, Inc., Rochester Gas and Electric Corporation, and National Fuel Gas Distribution Corporation (collectively the "Joint Utilities") submit this request for clarification of the New York State Public Service Commission's ("Commission") *Order Establishing Oversight Framework and Uniform Business Practices for Distributed Energy Resource Suppliers* ("Order").[1]

The Order established Uniform Business Practices ("DERS-UBPs") that apply to distributed energy resource suppliers ("DERS"), a group of entities broadly defined as "a supplier of one or more DERs that participates in a Commission-authorized and/or utility or

[1] Case 15-M-0180, *In the Matter of Regulation and Oversight of Distributed Energy Resource Providers and Products* ("DER Oversight Proceeding"), Order Establishing Oversight Framework and Uniform Business Practices for Distributed Energy Resource Suppliers ("Order")(issued October 19, 2017).

DSP-operated program or market."[2] The establishment of the DERS-UBPs is an important step toward providing much needed guidance and consistency to both utilities and DERS operating in New York State.

The Order and the DERS-UBPs discuss a preference of DERS transacting and obtaining data from the Joint Utilities through the Electronic Data Interchange ("EDI"), which has long been used primarily by the Joint Utilities and energy services companies ("ESCOs"). The Order, however, does recognize that there are other methods and platforms for sharing customer data, and that the requirements and policies associated with receiving data through these systems "will be developed in those venues."[3]

Section 2C of the DERS-UBPs establishes requirements related to DERS access and use of customer data, including requirements for obtaining customer consent. Section 2C, however, applies only to DERS obtaining data through EDI, and specifically does not apply to other either existing or planned platforms for receiving customer data. This limitation is a cause for concern and the Joint Utilities respectfully request the Commission to clarify that Section 2C of the DERS-UBPs apply to DERS who are seeking to obtain customer data regardless of the utility platform that the DERS will be requesting the data so that the necessary rules for obtaining consent, among other things, apply across all platforms. The importance of DERS obtaining and retaining required customer consent before requesting data from the Joint Utilities cannot be understated. Equally important are the requirements in Section 2C, Subparts (E), (F), and (G) related to unauthorized release of customer data, the prohibition against selling or disclosing customer data, cybersecurity, and the need to comply with any utility or Commission data security requirements. Applying the customer data requirements broadly to DERS regardless of

[2] UBPs, p. 1.
[3] DER Oversight Proceeding, Order, p. 28.

the data platform will provide essential protections to customers and Commission oversight over DERS. This is especially important because the DERS-UBPs for most DERS do not call for any Commission registration or vetting process, yet will still require the Joint Utilities to provide highly customer-specific data points to any DERS and to presume that the DERS properly obtained the customer's consent.

Therefore, the Joint Utilities respectfully request that the Commission clarify that Section 2C, Subparts (A), (B), (D), (E), (F), and (G) apply to DERS requesting customer data not only through EDI, but also include other utility platforms for data access.[4]

[4] Section 2C, Subpart (C) is not included in this request because other data exchange platforms may not provide the same data points as required by the DERS-UBPs through EDI.

STATE OF NEW YORK
PUBLIC SERVICE COMMISSION

In the Matter of Regulation and Oversight of Distributed Energy Resource Providers and Products	**Case 15-M-0180**
Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place	**Case 18-M-0376**

JOINT UTILITIES RESPONSE TO MISSION:DATA PETITION FOR DECLARATORY RULING

I. Introduction

Pursuant to 16 NYCRR 8.2(c), Central Hudson Gas & Electric Corporation, Consolidated Edison Company of New York, Inc. ("Con Edison"), New York State Electric & Gas Corporation, Niagara Mohawk Power Corporation d/b/a National Grid, KeySpan Gas East Corporation d/b/a National Grid and The Brooklyn Union Gas Company d/b/a National Grid NY (collectively, "National Grid"), Orange and Rockland Utilities, Inc., and Rochester Gas and Electric Corporation (collectively the "Joint Utilities") for the reasons below urge the New York Public Service Commission ("Commission") to dismiss Mission:data Coalition's ("Mission:data") Petition ("Petition") seeking a declaratory ruling to prohibit the Joint Utilities from requiring Distributed Energy Resources ("DERs") registering to use Green Button Connect My Data® ("GBC"), or

similar electronic interface,[1] to comply with certain data security and privacy requirements.[2] The Commission just initiated a new proceeding to comprehensively evaluate access to customer energy data in its *Order Adopting Accelerated Energy Efficiency Targets* ("EE Order").[3] In the EE Order, the Commission directed Department of Public Service Staff ("Staff") to convene a collaborative with interested stakeholders specifically to develop a GBC terms and conditions agreement to be filed by the Joint Utilities by February 29, 2019.[4] Mission:data's Petition is moot because the Joint Utilities will be working with Staff and interested stakeholders, including presumably Mission:data, to develop appropriate GBC cyber security and customer data protections. Accordingly, the Mission:data Petition should be dismissed.

In the alternative, the Petition should be dismissed on substantive grounds because the Joint Utilities have an obligation to protect their systems and customer data privacy, including requiring appropriate safeguards and protections from third parties, and nothing in the Commission's Uniform Business Practices ("UBPs") DERs Order[5] prohibits imposing requirements on third parties. As shown below, the Joint Utilities' requirements are reasonable, routine non-disclosure agreement provisions, and in line with utilities in other states' requirements for third-party GBC users. The Joint Utilities recognize the inherent challenge in striking the right balance between protecting utility systems and customer data and animating third-party markets. It is vital that the

[1] Some utilities have not adopted GBC but provide the same information through a web portal.
[2] This also responds to comments filed by Mission:data on October 16, 2018 in Case 15-M-0180, *In the Matter of Regulation and Oversight of Distributed Energy Resource Providers and Products* ("DERs Proceeding").
[3] Case 18-M-0094, *In the Matter of a Comprehensive Energy Efficiency Initiative*, Order Adopting Accelerated Energy Efficiency Targets (issued December 13, 2018)("EE Order").
[4] The Joint Utilities will submit the GBC terms and conditions March 1, 2019.
[5] DERs Proceeding, Order Establishing Oversight Framework and Uniform Business Practices for Distributed Energy Resource Suppliers (issued October 19, 2017)("DERs UBP Order").

Commission establish appropriate cyber security and data protection requirements for third parties at the outset rather than just reacting to address cyber security issues, including losses or breaches, after they occur. Importantly, Staff recently issued a report recommending that DERs immediately comply with the each of the Joint Utilities' data security requirements to the extent they are interfacing with the Joint Utilities' systems in ways similar to the electronic data interchange ("EDI") interface.[6]

II. Procedural Background

The Joint Utilities have long required non-disclosure agreements ("NDA") or data security agreements ("DSAs") from third parties and contractors that receive customer data or that have access to utility systems. As pointed out in the EE Order, the Joint Utilities routinely share information with contractors and energy efficiency providers pursuant to agreements that contain appropriate safeguards.[7] NDAs and DSAs are the means of establishing appropriate safeguards. In addition, the Joint Utilities have entered into agreements with state entities like the New York State Energy Research and Development Authority ("NYSERDA"), contractors, and countless other third parties that are either interacting with utility systems or receiving customer data. These types of agreements, whether titled NDAs, DSAs, or terms and conditions, are routine, and a necessity of doing business when exchanging customer and other sensitive data. The specific

[6] Case 18-M-0376, *Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place* ("Cyber Security Proceeding"), Department of Public Service Staff Report on the Status of the Business-to-Business Collaborative to Address Cyber Security in the Retail Access Industry (filed September 24, 2018)("Staff Report").
[7] EE Order, p. 43.

terms and conditions of these types of agreements have generally been similar, with modifications over the years to keep pace with rapidly evolving technology and cyber security risks. The Joint Utilities have generally negotiated these agreements without the Commission's review or approval.

Consistent with the Commission's decision that "[p]rotection of consumer information is a basic tenet of the Public Service Law and our policies"[8] and its determination to approve a vendor contract, in part, because "we have had an opportunity to review the contract between the utility and [the vendor] and believe it offers sufficient privacy safeguards because the agreement prohibits customer information and usage data from being used for any purpose other than to administer the program and *the agreement provides for the indemnification of the utility* in the event of a breach or non-compliance of the agreement"[9] the Commission has approved the use of DSAs. Within the context of expediting community choice aggregation ("CCA") programs, the Commission approved a specific form of a DSA.[10] CCA administrators are required to sign the DSA in order to receive a list of customer names and addresses in the CCA area in order to administer opt-out letters. Additionally, the Commission recently approved of the process resulting in a negotiated DSA executed between the Joint Utilities and Energy Service Companies ("ESCO") and others.[11]

---

[8] Cases 07-M-0548 *et al*., *Proceeding on Motion of the Commission Regarding an Energy Efficiency Portfolio Standard* ("EEPS Proceeding"), (Order on Rehearing Granting Petition for Rehearing (issued December 3, 2010) ("OPower Order"), p. 17.

[9] *Id*., pp. 17-18 (emphasis added).

[10] Cases 14-M-0224 *et al*., Proceeding on Motion of the Commission to Enable Community Choice Aggregation Programs, *Order Approving Community Choice Aggregation Program and Utility Data Security Agreement with Modifications* (issued October 19, 2017).

[11] Cyber Security Proceeding, Order Instituting Proceeding (issued June 14, 2018).

In short, there has been a consistent practice by the Joint Utilities, reflecting industry best practices, and acknowledgement by the Commission, that safeguards are necessary to protect the utilities' systems and customer data.

Similarly, within the Reforming the Energy Vision ("REV") Proceeding,[12] the Commission has identified a need to have oversight, including oversight related to customer data, over third parties as markets develop. In its *Order Adopting Regulatory Policy Framework and Implementation Plan* ("REV Track One Order"),[13] the Commission concluded that a degree of oversight over DERs would be necessary "to ensure both consumer protection and fair competition,"[14] and stated that it would take "an active role in establishing and enforcing consumer protections related to DER providers."[15] To initiate the development of the DERS oversight process, the Commission directed Staff to develop standards in consultation with stakeholders.[16] Staff issued proposed Uniform Business Practices ("UBP") for DERs for which the Commission sought public comment.[17] The Joint Utilities and many other stakeholders submitted initial and reply comments.

Thereafter, in its March 9, 2017 *Order on Net Energy Metering Transition, Phase One of*

[12] Case 14-M-0101, Proceeding on the Motion of the Commission in Regard to Reforming the Energy Vision ("REV Proceeding").
[13] *Id.*, Order Adopting a Regulatory Policy Framework and Implementation Plan (issued February 26, 2015)("REV Track One Order").
[14] *Id.*, p. 102.
[15] *Id.*, p. 104.
[16] Id., p. 105.
[17] DERs Proceeding, Staff Proposal (filed July 28, 2015).

Value of Distributed Energy Resources, and Related Matters ("VDER Phase One Order"),[18] the Commission directed Staff to file an updated whitepaper on oversight of DERs. On April 11, 2017, Staff filed its Supplemental Staff Whitepaper on DER Oversight, along with updated UBPs.[19] The Joint Utilities and interested stakeholders, including Mission:data, again submitted comments. On October 19, 2017, the Commission established oversight over DERs and adopted a set of DERs UBPs.[20]

The DERs UBP Order and UBP-DERs established a preference for DERs to request and receive data from the Joint Utilities through EDI, which has traditionally been used between the Joint Utilities and ESCOs. The Commission, nonetheless, recognized that there are other methods and platforms for sharing customer data, and that the requirements and policies, including cyber and customer data protections, associated with receiving data through these systems "will be developed in those venues."[21] Until the Commission develops methods to regulate other methods and platforms, the Commission recognized and determined that:

> [T]he UBP-DERS will not apply to transactions between a DER supplier and a utility or other program administrator. *Rules governing behavior* in and oversight of those programs and transactions *will appear within the program rules, the utility tariff, or the procurement request or contract*, though the Commission may consider standardization of such rules into the UBP-DERS in the future.[22]

---

[18] Cases 15-E-0751 *et al*., *In the Matter of the Value of Distributed Energy Resources* ("VDER Proceeding"), Order on Net Energy Metering Transition, Phase One of Value of Distributed Energy Resources, and Related Matters (issued March 9, 2017) ("VDER Phase One Order").
[19] DERs Proceeding, Supplemental Staff Whitepaper on DER Oversight (filed April 11, 2017)("Updated UBP-DERs Staff Whitepaper").
[20] DERs Proceeding, DERs UBP Order.
[21] *Id.*, p. 28.
[22] *Id*. p. 18 (emphasis added).

Section 2C of the UBP-DERs established specific requirements related to DERs access and use of customer data through EDI and notes that those requirements do not apply to other either existing or planned platforms for receiving customer data. Consistent with the DERs UBP Order, requirements related to access and use of customer data through other platforms, like GBC, would be developed elsewhere, including contracts between the DERs and the applicable utility. On November 21, 2017, the Joint Utilities requested that the Commission clarify that Section 2C, Subparts (A), (B), (D), (E), (F), and (G) apply to DERs requesting customer data not only through EDI, but also including other utility platforms for data access ("Request for Clarification").[23]

The Joint Utilities explained that Section 2C should apply to DERs regardless of platform because the risk of harm to utility systems and/or loss of sensitive customer data is the same. The Joint Utilities sought clarification because, as a matter of convenience, consistency and efficiency, the customer data access requirements should be encompassed in the one document – in this case, the UBP-DERs. Separate requirements, or requirements contained in different documents developed in different proceedings, where the risk of harm to systems or data loss is the same, is inefficient and confusing to market participants. If the risk to systems and potential damage of data loss is either the same or similar across platforms, the requirements should be the same and consolidated in one place. More important, the fact that the Commission has indicated that requirements for non-EDI platforms would be developed elsewhere, however, does not mean that

[23] *See* DERs Proceeding, Joint Utilities' Request for Clarification (filed November 2, 2017). Subpart (C) is not included in this request because other data exchange platforms may not provide the same data points as required by the UBPs through EDI.

there should be no requirements for access to data through those platforms, and the Joint Utilities properly continue to require NDAs or DSAs, as the Commission intended, where appropriate to protect their systems and customer data.[24]

Since the Joint Utilities' Request for Clarification was filed, the importance of having appropriate data privacy and cyber security protections in place for the Joint Utilities and third-party DERs has increased as high profile cyber and data breach incidents become increasingly common.[25] For example, in June 2018, following a significant energy services market cyber incident that impacted hundreds of thousands of New York customers, the Commission instituted a proceeding to determine appropriate cyber security and data privacy protocols for a variety of energy services entities ("ESEs"), including ESCOs and, importantly, DERs.[26]

After extensive collaboration with Staff, the Joint Utilities, and a variety of stakeholders,[27] including EDI providers, ESCOs, large direct customers, and state agencies, a DSA and an accompanying cyber-security self-attestation ("Attestation") were developed, posted on the Staff-administered cyber security website for comment, and sent to ESEs. Together, the DSA and Attestation establish appropriate cyber security and customer data protection rules for utilities and

[24] The Commission has not acted on the Joint Utilities' Request for Clarification.
[25] https://www.businessinsider.com/data-hacks-breaches-biggest-of-2018-2018-12#21-british-airways-380000-1
[26] Cyber Security Proceeding, *Order Instituting Proceeding* (issued June 14, 2018).
[27] The Commission requested that the Parties conduct a "business to business" process to develop the DSA and Attestation. As a result, there were three in-person meetings, including two days discussing the ESCOs issues with the DSA and numerous phone calls among the parties. Interested stakeholders provided comments on the DSA and the Attestation, and the Joint Utilities lessened the requirements of the DSA and the Attestation on several occasions. The Joint Utilities requested that Attestations be provided by August 18, 2018 and signed DSAs by August 31, 2018.

ESEs participating in New York energy markets to protect their respective systems and customer data.

Critically, the DSA[28] imposes mutual obligations upon the Joint Utilities and the energy services entities to protect confidential customer data. On September 24, 2018, Staff issued its Staff Report.[29] Staff concluded that the end result of the cyber security business-to-business process was a DSA developed from the Joint Utilities' original proposal that "strikes a fair balance between the Joint Utilities' concerns of both protecting the utility systems from infiltration and against customer data breaches, and the ESE's concerns of overreaching and over-burdensome cyber security requirements."[30] The Staff Report also stated that the "Self-Attestation consists of a 16-point inventory of cyber controls based on National Institute of Standards and Technology ("NIST") standards, and requested that ESCOs and ESEs attest that they observe these minimum standards, or if the ESE is not already doing so, to implement these controls within a reasonable timeframe."[31]

A significant number of entities have already signed the DSA and submitted the Attestation. In addition, with respect to ESCOs, the Joint Utilities also filed a Petition for Declaratory Ruling[32] with the Commission seeking confirmation that each utility can discontinue

[28] The Joint Utilities used the Commission's approved DSA developed for CCA administrators as a template.
[29] Cyber Security Proceeding, *supra* note 6.
[30] *Id*., pp. 4-5.
[31] *Id*., p. 5.
[32] Cyber Security Proceeding, Petition of the Joint Utilities for Declaratory Ruling Regarding their Authority to Discontinue Utility Access to Energy Service Companies in Violation of the Uniform Business Practices (filed November 9, 2018)("Petition for Declaratory Ruling"). A revised version of the Petition for Declaratory Ruling was filed the same day.

an ESCO's participation in its retail access program for failure to meet minimum data security standards pursuant to the Commission's UBP requirements for ESCOs.

Due to potential differences between ESCOs and some DERs, the Staff Report recommended a similar business-to-business process to "refine the existing DSA to make its terms more aptly applicable to DERS." Importantly, Staff goes on to recommend, in the interim, application of the revised DSA to DERs with EDI type interfacing as the most appropriate articulation of cyber controls to be applied to this industry.[33] Staff specifically recommends that DERs comply with UBP Section 2(C)(g), which states:

> DER suppliers that obtain customer information from the distribution utility or DSP must comply with any data security requirements imposed by that utility or by Commission rules on ESCOs and/or any data security requirements associated with EDI eligibility.

On November 14, 2018, Staff held a collaborative meeting with interested stakeholders to discuss revisions to the DSA and Attestation. Comments on the DSA and Attestation were submitted on December 14, 2018. Some commenters opposed the imposition of any data security requirements[34] and others recommended specific modifications to the DSA and/or Attestation. The Joint Utilities are in the process of reviewing all comments, and will identify further reasonable changes, if any, to the DSA as appropriate. While it is unclear how this ongoing process will blend with the new collaborative under the EE Order, because of the significant overlap

[33] *Id.*, p. 8.

[34] Interestingly, many of the comments start off by explaining the need for cyber security but then try to distinguish why DERS are different. Not one of the comments has shown that they are different and do not require cybersecurity controls.

between the ongoing process in the Cyber Security Proceeding and the EE Order, the Joint Utilities recommend that the work already completed in the Cyber Security Proceeding be combined with and incorporated into the new proceeding and collaborative process stemming from the EE Order. The Joint Utilities expect that, following this collaborative, a DSA and Attestation can be finalized that will apply to all DERs, regardless of the platform the DER is using to access data. This will provide consistency, ease of administration, and certainty for DERs and protect utility systems and customer data.

III. Mission:data Ignores the Commission's Clear Policies Requiring the Protection of Utility Systems and Customer Data

GBC is an industry-developed nationwide tool that allows customers to easily authorize registered third parties to receive access to their customer usage data based on affirmative (opt-in) customer consent and control. GBC provides a reliable protocol for customer authorization, data transfer, data formatting, and data exchange. The protocol leverages modern technical applications.

Con Edison has developed GBC (known as "Share My Data"). Contrary to Mission:data's inaccurate assertion,[35] the first phase of Con Edison's implementation of Share My Data is complete and several third-party DERs are at various stages of the onboarding process. In fact,

[35] This is one of many misstatements both in Mission:data's comments and presentation provided at the November 14, 2018 meeting. Mission:data's statement that Share My Data will not "go live" until January 2019 is incorrect, and Mission:data may have been confusing the second phase of the Share My Data project with the initial "go live." Con Edison's Phase 2 Report (filed October 2, 2017) detailed the timeline and considerations related to expanding the data sets available through Share My Data.

one DER has completed the process and customers now have the option in their My Account web portal to utilize the Share My Data feature and have their usage information shared with a registered third party. Another DER is currently in the final technical implementation phase. Con Edison requires third parties registering to obtain data through Share My Data to sign the DSA and complete the Attestation. Eight third parties have submitted DSAs.[36]

The Joint Utilities take seriously their responsibility to protect utility systems and customer data. The Commission too has continued its policy of stressing the importance of cyber security and customer privacy.[37] For instance, in the REV Track One Order, the Commission stated the following regarding the importance of cyber security: "Cyber security is highly important for reasons of privacy, reliability, resiliency and market confidence. It needs to be designed and built into utility systems including the DSP."[38] Importantly, the Commission went on to emphasize that security methods, systems and protocols require constant vigilance and reassessment, with new vulnerabilities being discovered and exploited, and new countermeasures developed and implemented.[39]

[36] Prior to the Cyber Security Proceeding Staff-led collaborative, the Joint Utilities' IT assessments were more robust checklists that third parties needed to fill out and return to the utility. Based on feedback during the collaborative, and the desire of third parties to a consistent process among the Joint Utilities, the Joint Utilities streamlined the requirements which are based on the NIST framework, and permitted the third party to have an officer attest that they had the required controls in place. This shortened form is the Attestation discussed in Section II above.
[37] *See* EEPS Proceeding, OPower Order.
[38] REV Proceeding, REV Track One Order, p. 99.
[39] Id., p. 100.

In its *Order Adopting Distributed System Implementation Plan Guidance*, the Commission clearly articulated the importance the customer data privacy and the security of utility systems by stating:

> [w]hile planning and operations must become more visible and transparent, ensuring customer privacy, as well as system security and reliability, remain paramount. In an increasingly technological world, protection of consumer information, privacy, cybersecurity, and physical security are subjects that require constant vigilance, improvement, and adaptation.[40]

More recently, in the Cyber Security Order, the Commission raised concerns about a recent retail market cyber incident and recognized that cyber security threats are becoming more common and that industry must be vigilant in order to protect against, detect, and respond to these events.[41] The Commission went on to state: "[i]t is essential to ensure that cyber security protections are being adequately addressed to mitigate vulnerability of utility systems to cyber-attacks, and to ensure that confidential and sensitive customer information remains safeguarded from potential data breaches."[42]

In addition to the importance of appropriate cyber security protections, the Commission also has a longstanding policy of maintaining the privacy of customer information, including usage information. The Commission's OPower Order clearly articulated the need for the customer data privacy. The Commission stated: "Protection of consumer information is a basic tenet of the Public Service Law and our policies."[43] The Commission has repeatedly required explicit customer

[40] REV Proceeding, Order Adopting Distributed System Implementation Plan Guidance ("DSIP Guidance Order") (issued April 20, 2016), pp. 2-3.
[41] Cyber Security Proceeding, Cyber Security Order, p. 2.
[42] *Id.*, p. 3.
[43] EEEPS Proceeding, *supra* note 8, p. 17.

consent for ESCOs, DERs, and other third parties to obtain customer usage data. In addition to consent, as discussed above, the Commission has established guidelines and policies for DERs and ESCOs to keep information they receive from a customer confidential, not to sell it, or disclose without explicitly informing the customer.[44] The Commission also requires the Joint Utilities to have a third party complete an annual assessment of utility practices, systems and programs to protect customer personally identifiable information.[45] Finally, the Commission's *Order Adopting a Ratemaking and Utility Revenue Model Policy Framework* ("REV Track Two Order")[46] makes clear that third parties, including DERs, are required to protect customer-specific information.

In short, the Commission has been emphatic on the importance of the Joint Utilities and third parties having appropriate requirements in place for cyber security and data privacy. Mission:data is incorrect that there is no need for cyber-security or customer data protections if the customer actively chooses to send third parties their data. In support of its position that such requirements are not necessary where consent need not be presumed, Mission:data relies on a selective reading of the Joint Utilities' Request for Clarification that deals with consent. Mission:data disregards the Joint Utilities concerns related to requirements associated with the unauthorized release of customer data, the prohibition against selling or disclosing customer data, cybersecurity, and the need to comply with any utility or Commission data security requirements. In disregarding those concerns, Mission:data also disregards the Commission's clear focus on the

[44] UBP-DERs, Section 2(E), ESCO UBPs Section 4(F).
[45] Case 13-M-0178, In the Matter of a Comprehensive Review of Security for the Protection of Personally Identifiable Customer Information, *Order Directing the Creation of an Implementation Plan* (issued August 19, 2013).
[46] REV Proceeding, Order Adopting a Ratemaking and Utility Revenue Model Policy Framework (issued May 19, 2016")("REV Track Two Order"), p. 145.

need for appropriate safeguards of utility systems and customer data regardless of whether customer consent is presumed or not.

Without executed DSAs and Attestations, the Joint Utilities and their customers are exposed to cyber security risks, including customer data loss and financial risk. These risks include the ability of DERs to harm a utility system during the regular exchange of information as well as the potential loss of customer data. This risk exists not only using the EDI platform, but also other electronic data platforms, including GBC. The US Department of Energy implicitly recognizes that GBC poses cyber security risks by designing it in compliance with Energy Services Provider Interface ("ESPI") data standard released by the North American Energy Standards Board ("NAESB") and the National Institute of Standards and Technology ("NIST")[47] and making GBC comply with "current privacy and security practices." Moreover, third parties must be required to have policies and protocols to protect the data they receive from unauthorized release, as well as other provisions to protect the Joint Utilities in the event of a breach caused by a third party.

The DSA and Attestation represent the minimum requirements that third parties should have to protect their systems, utility systems, and customer information, not the maximum. The requirements were developed and refined after receiving extensive input from interested stakeholders. Staff has found them to be reasonable and convened the November 14, 2018 collaborative only to determine whether certain refinements are necessary based on inherent differences between ESCOs and DERs. During the collaborative, several stakeholders emphasized

[47] US Department of Energy Green Button Open Energy Data, pp. 5-6, available at https://www.energy.gov/data/green-button

that the DERs DSA and Attestation requirements for DERs should be the same between ESCOs and DERs.

The new collaborative to effectively bring these issues together notwithstanding, the Commission has explained that cyber security and data privacy protections are vital for utilities and third parties. The Joint Utilities believe the collaboratively-developed DSA and Attestation strike a fair balance between customer and utility protections and third-party needs.

IV. The Joint Utilities Are Permitted to Require DSAs and Attestations

First, the UBPs applicable to DERs do not prohibit the Joint Utilities from imposing any requirements for third party access to GBC. The fact that the UBP- DERs have a section establishing requirements for DERs using EDI does not mean that DERs using other platforms can do so without any requirements. In fact, the DERs UBP Order acknowledged that there would be requirements for access to data through other platforms,[48] and that in the meantime program rules, utility tariffs, and contracts would govern.[49] While the Joint Utilities requested clarification of the UBP-DERs, that request in no way precludes the Joint Utilities from requiring DSAs and Attestations. The Joint Utilities requested clarification so that there would be consistent requirements among all third parties accessing data from Joint Utilities. The Joint Utilities believe that REV market participants would prefer consistency, especially considering the fact that an

[48] DERs Proceeding, DERs UBP Order, p. 28.
[49] *Id*. p. 18.

entity could be providing several different types of services. The Commission should reject Mission:data's argument that, because Section 2 of the UBP-DERs applies only to EDI, the Joint Utilities are not permitted to require any cyber security or customer data protections as a prerequisite to third party use of GBC.[50]

V. The DSA and SA Align with Other State's Cyber Security and Data Privacy Requirements

At the November 14, 2018 collaborative to discuss refinements to the DSA and Attestation, Mission:data incorrectly represented that there are little, and in some cases, no cyber security and data protection requirements required in other states that are in the process, or have already, implemented GBC. For instance, Mission:data suggested that California required only "reasonable safeguards" and Illinois required "none, other than non-disclosure.[51] However, even a cursory review of requirements in those and other states demonstrates that the requirements for third parties to use GBC are far more robust than that presented by Mission:data.

Commonwealth Edison in Illinois, for example, has a data services handbook for third parties that includes a detailed description of how to register for GBC. As part of the registration process, third parties are required to sign what appears to be a robust NDA as well as a data access and retrieval form.[52] Based on the only page of the NDA visible in the handbook, it appears the

[50] The Joint Utilities also acknowledge that several other DERs have submitted comments in the Cyber Security Proceeding making the same argument.
[51] Mission:data PowerPoint presentation from November 14, 2018 collaborative, s. 6.
[52] https://www.comed.com/SiteCollectionDocuments/SmartEnergy/ADSHandbook.pdf

definition of what is considered confidential information is similar, if not broader than the definition used in the DSA. There are also clear provisions relating to data loss or breach and the ability to seek monetary damages and/or injunctive relief – these provisions are akin to the types of provisions in the DSA.

The California Public Utility Commission ("CPUC") has developed strict customer data protection rules and standards for third parties. Third parties are subject to the Rules Regarding Privacy and Security Protections for Energy Usage Data adopted by the CPUC as Attachment D to Decision 11-07-056 (Electric).[53] The requirements of that lengthy decision are incorporated in California utility tariffs and terms and conditions for access to data using GBC. Specifically, Pacific Gas & Electric Company ("PG&E") has strict Customer Data Privacy and Protection Rules requirements included in PG&E's Customer Data Access Tariff.[54] In addition to the Rules and tariff, PG&E also has extensive terms and conditions specific to GBC.[55] PG&E's terms and conditions for third party use of GBC include many of the same requirements as the DSA. The terms and conditions include a broad indemnity, warranties, limitations on liability in favor of the utility, and insurance. In addition, like the DSA, the terms and conditions apply not only to the third party registering to use GBC, but also to their agents, contractors and subcontractors.

Therefore, Mission:data's suggestion that other states have little or no requirements for third-party access to GBC is inaccurate. In fact, as shown above, a review of other state and utility

[53] http://docs.cpuc.ca.gov/PUBLISHED/FINAL_DECISION/140369.htm
[54] https://www.pge.com/tariffs/tm2/pdf/ELEC_4378-E-A.pdf
[55] https://www.pge.com/includes/docs/pdfs/myhome/addservices/moreservices/sharemydata/ShareMyData_Platform_TermsofUse.pdf

requirements only supports that the Joint Utilities are in line with other GBC implementation, and that throughout the country commissions, utilities, and third parties recognize the importance of cyber security and customer data protection.

The Joint Utilities look forward to continued discussions in the collaborative established in the EE Order. Indeed, the EE Order specifically states that terms and conditions, including customer privacy agreements, should be used as a reference in developing GBC agreements in New York. The Joint Utilities believe the existing DSA and Attestation closely aligns with the policies of other states, which all recognize the need for agreements that appropriately protect utility systems and customer energy usage data.

VI. Conclusion

Mission:data's Petition should be dismissed based on the issues discussed herein. The Joint Utilities are permitted to require third parties to comply with minimum data security and customer data protection requirements. Moreover, Mission:data's Petition has been effectively superseded by the new collaborative taking place as a result of the EE Order, which acknowledges the need for cyber security and data protections. The Commission should confirm the Joint Utilities' ability to require compliance during the pendency of the collaborative discussions.

THE WALL STREET JOURNAL

https://www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112?mod=searchresults&page=1&pos=1[wsj.com]

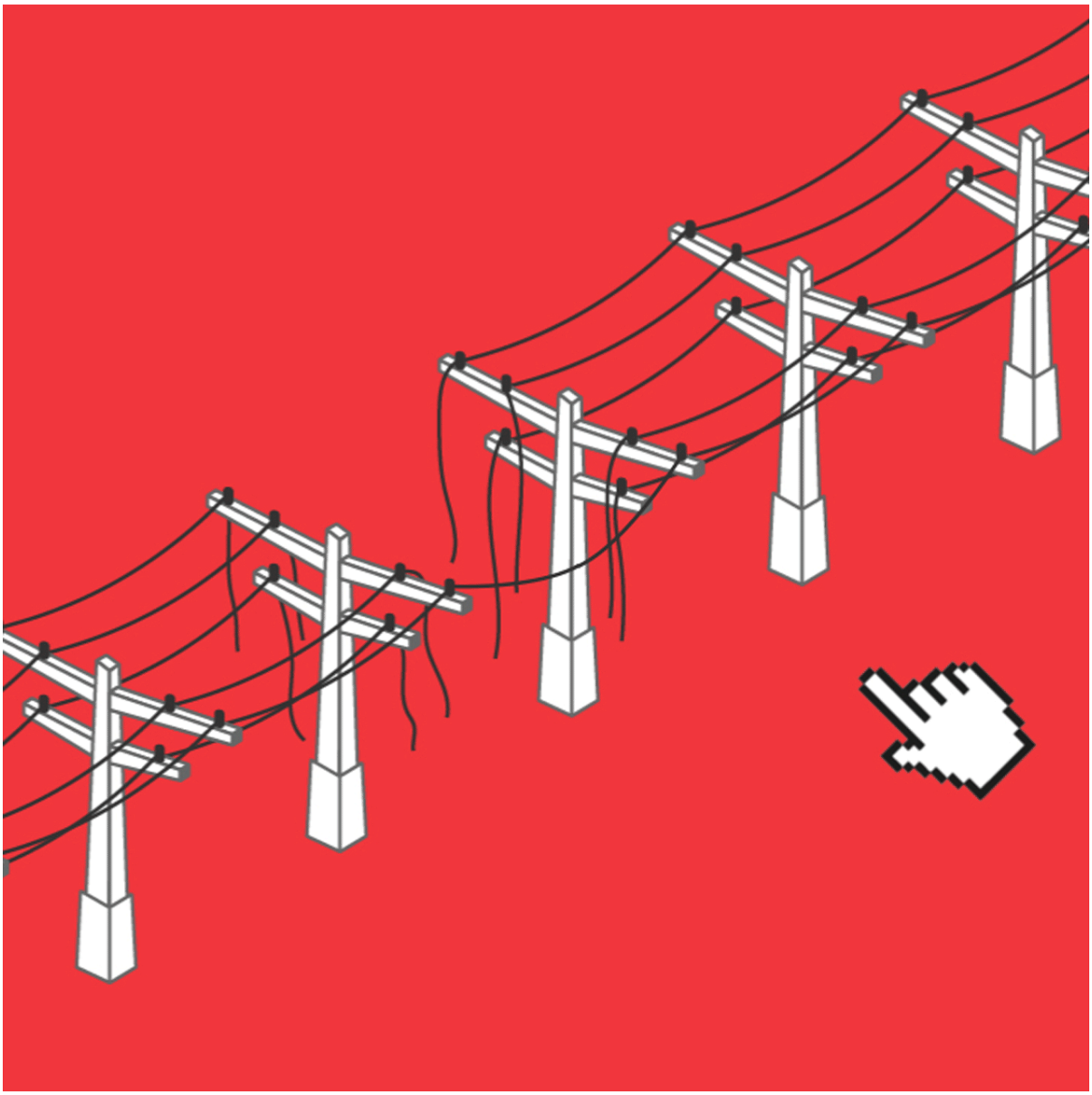
America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It

A Wall Street Journal reconstruction of the worst known hack into the nation's power system reveals attacks on hundreds of small contractors

By
Rebecca Smith and
Rob Barry

Jan. 10, 2019

...



One morning in March 2017, Mike Vitello's work phone lighted up. Customers wanted to know about an odd email they had just received. What was the agreement he wanted signed? Where was the attachment?

Mr. Vitello had no idea what they were talking about. The Oregon construction company where he works, All-Ways Excavating USA, checked it out. The email was bogus, they told Mr. Vitello's contacts. Ignore it.

Then, a few months later, the U.S. Department of Homeland Security dispatched a team to examine the company's computers. You've been attacked, a government agent told Mr. Vitello's colleague, Dawn Cox. Maybe by Russians[wsj.com]. They were trying to hack into the power grid.

“They were intercepting my every email,” Mr. Vitello says. “What the hell? I’m nobody.”

“It’s not you. It’s who you know,” says Ms. Cox.

The cyberattack on the 15-person company near Salem, Ore., which works with utilities and government agencies, was an early thrust in the worst known hack by a foreign government into the nation’s electric grid[wsj.com]. It set off so many alarms that U.S. officials took the unusual step in early 2018 of publicly blaming the Russian government.

A reconstruction of the hack reveals a glaring vulnerability at the heart of the country’s electric system. Rather than strike the utilities head on, the hackers went after the system’s unprotected underbelly—hundreds of contractors and subcontractors like All-Ways who had no reason to be on high alert against foreign agents. From these tiny footholds, the hackers worked their way up the supply chain. Some experts believe two dozen or more utilities ultimately were breached.[wsj.com]

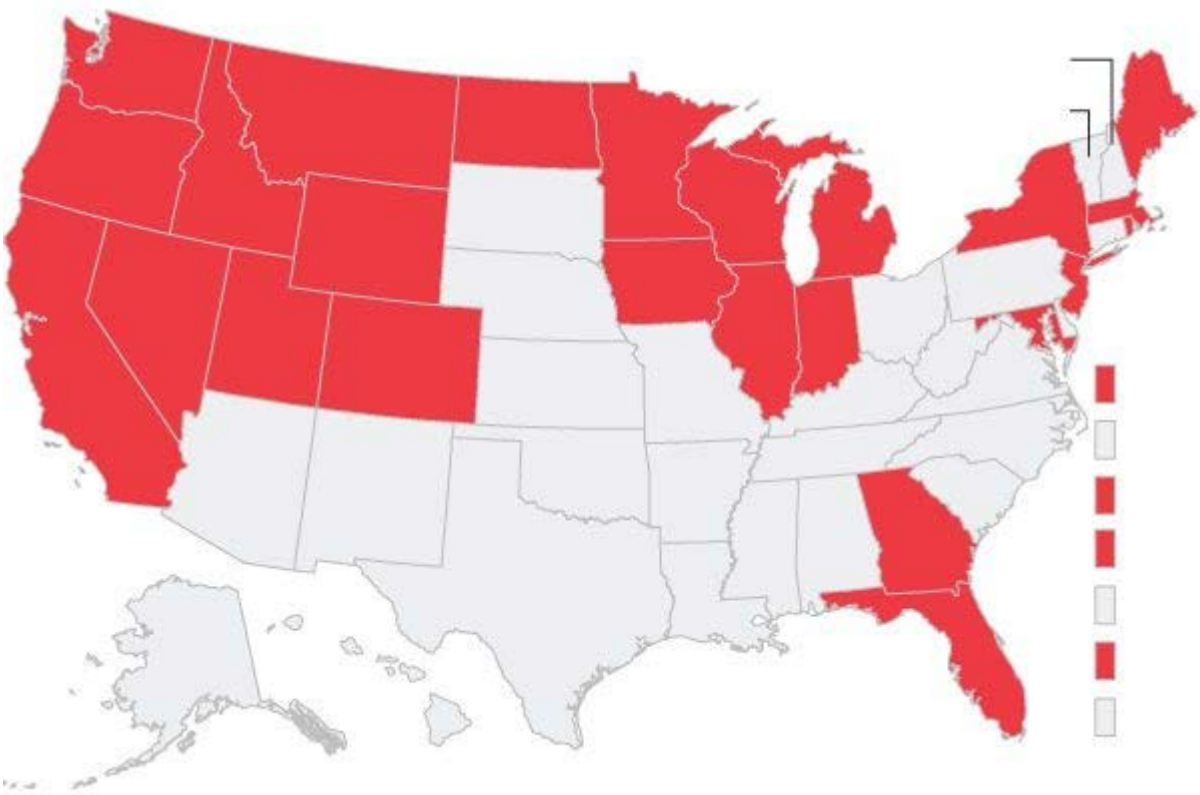
The scheme’s success came less from its technical prowess—though the attackers did use some clever tactics—than in how it exploited trusted business relationships using impersonation and trickery.

The hackers planted malware on sites of online publications frequently read by utility engineers. They sent out fake résumés with tainted attachments, pretending to be job seekers. Once they had computer-network credentials, they slipped through hidden portals used by utility technicians, in some cases getting into computer systems that monitor and control electricity flows.

The Wall Street Journal pieced together this account of how the attack unfolded through documents, computer records and interviews with people at the affected companies, current and former government officials and security-industry investigators.

In the Crosshairs

Russian hackers seeking to infiltrate the power grid targeted companies operating in at least 24 states, Canada and the U.K.



NH

Source: documents; interviews with people at the affected companies, government officials and security-industry investigators

The U.S. government hasn't named the utilities or other companies that were targeted. The Journal identified small businesses such as Commercial Contractors Inc., in Ridgefield, Wash., and Carlson Testing Inc., in Tigard, Ore., along with big utilities such as the federally owned Bonneville Power Administration and Berkshire Hathaway[quotes.wsj.com] 's PacifiCorp. Two of the energy companies targeted build systems that supply emergency power to Army bases.

The Russian campaign[wsj.com] triggered an effort by the Federal Bureau of Investigation and Homeland Security to retrace the steps of the attackers and notify possible victims. Some companies were unaware they had been compromised until government investigators came calling, and others didn't know they had been targeted until contacted by the Journal.

"What Russia has done is prepare the battlefield without pulling the trigger[wsj.com]," says Robert P. Silvers, former assistant secretary for cyber policy at Homeland Security and now a law partner at Paul Hastings LLP.

The press office at the Russian Embassy in Washington didn't respond to multiple requests for comment. Russia has previously denied targeting critical infrastructure.

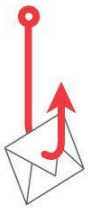
Early victims

In the summer of 2016, U.S. intelligence officials saw signs of a campaign to hack American utilities, says Jeanette Manfra, assistant secretary of Homeland Security's cybersecurity and communications program. The tools and tactics suggested the perpetrators were Russian. Intelligence agencies notified Homeland Security, Ms. Manfra says.

In December 2016, an FBI agent showed up at a low-rise office in Downers Grove, Ill., less than an hour west of Chicago. It was home to CFE Media LLC, a small, privately held company that publishes trade journals with titles such as "Control Engineering" and "Consulting-Specifying Engineer."

Tools of the Trade

In cyberattacks against U.S. power utilities, Russian hackers stole employee credentials to gain access to corporate systems, U.S. officials say.



Spearphishing
Hackers sent emails with malicious links or attachments that helped steal the recipient's credentials.
Watering-Hole Attacks

Hackers planted malicious code on trusted websites such as trade publications that they hoped their targets would visit. The code recorded visitors' confidential information.

Remote Access

With the stolen credentials, the hackers used virtual private networks and remote desktop programs to stay hidden and maintain access to internal networks.

Source: Department of Homeland Security

According to a CFE email, the agent told employees that "highly sophisticated individuals" had uploaded a malicious file onto the website for Control Engineering. The agent warned it could be used to launch hostile actions against others.

Steve Rourke, CFE Media's co-founder, says his company took steps to fix the infected site. Before long, though, attackers laced other CFE Media trade publications with malicious content, according to security researchers at Accenture[quotes.wsj.com] 's iDefense unit and RiskIQ, a San Francisco cybersecurity company, who later analyzed details of the attack.

Like lions pursuing prey at a watering hole, the hackers stalked visitors to these and other trade websites, hoping to catch engineers and others and penetrate the companies where they worked. The Russians could potentially take down "anybody in the industry," says RiskIQ researcher Yonathan Klijnsma.

By planting a few lines of code on the websites, the attackers invisibly plucked computer usernames and passwords from unsuspecting visitors, according to government briefings on the attack and security experts who have reviewed the malicious code. That tactic enabled the Russians to gain access to ever more sensitive systems, said Homeland Security officials in industry briefings last year.

Mr. Vitello of All-Ways Excavating has no idea how the hackers got into his email account. He doesn't recall reading CFE's websites or clicking on tainted email attachments. Nonetheless, the intrusion was part of the Russian campaign, according to the security companies that studied the hack.

Russian hackers
CFE Media
All-Ways Excavating
Corvallis, Ore.-based firm
Commercial Contractors
Dan Kauffman Excavating

Carlson Testing
DeVange Construction
Power companies in New York and Wisconsin
2 Oregon power companies
3 U.K. companies
2 U.S. companies
Massachusetts power company
Sources: documents; interviews with people at the affected companies, government officials and security-industry investigators

On March 2, 2017, the attackers used Mr. Vitello's account to send the mass email to customers, which was intended to herd recipients to a website secretly taken over by the hackers.

The email promised recipients that a document would download immediately, but nothing happened. Viewers were invited to click a link that said they could "download the file directly." That sprang the trap and took them to a website called imageliners.com.

The site, registered at the time to Matt Hudson, a web developer in Columbia, S.C., was originally intended to allow people to find contract work doing broadcast voice-overs but was dormant at the time. Mr. Hudson says he had no idea Russians had commandeered his site.

The day the email went out—the same day Mr. Vitello's office phone lighted up in Oregon—activity on the voice-over site surged, with computers from more than 300 IP addresses reaching out to it, up from only a handful a day during the prior month. Many were potential victims for the hackers. About 90 of the IP addresses—the codes that help computers find each other on the internet—were registered in Oregon, a Journal analysis found.

Web developer Matt Hudson says he had no idea Russians had hacked into his site.

It isn't clear what the victims saw when they landed on the hacked voice-over site. Files on the server reviewed by the Journal indicate they could have been shown a forged login page for Dropbox, a cloud-based service that allows people to share documents and photos, designed to trick them into turning over usernames and passwords. It also

is possible the hackers used the site to open a back door into visitors' systems, giving them control over their victims' computers.

Once Mr. Vitello realized his email had been hijacked, he tried to warn his contacts not to open any email attachments from him. The hackers blocked the message.

Sneak Attack

Hackers sent bogus emails from the account of Oregon construction contractor Mike Vitello to herd recipients to a website they had secretly taken over, called imageliners.com. Hackers then used the site to seek access to contractors that do business with U.S. power utilities.

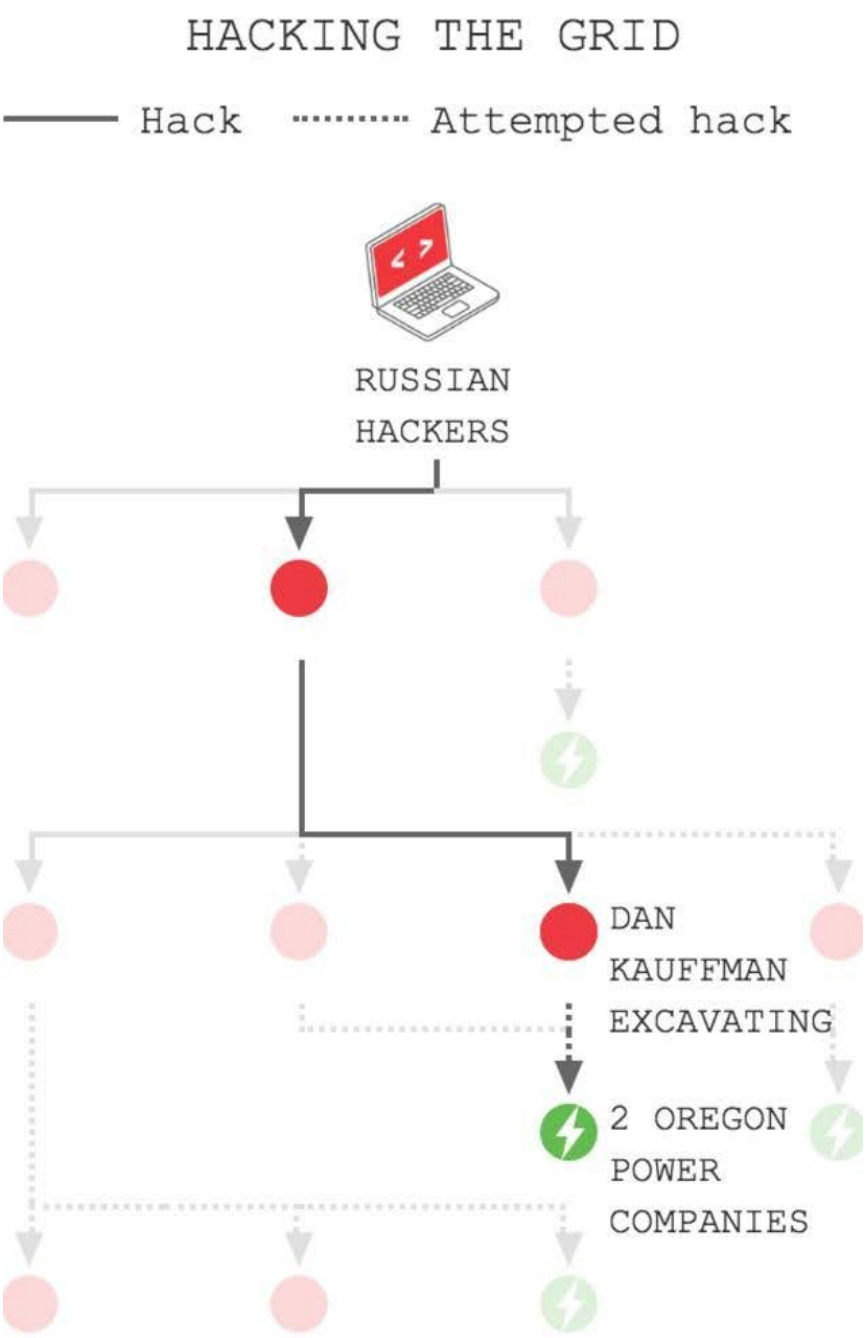
All-Ways Excavating is a government contractor and bids for jobs with agencies including the U.S. Army Corps of Engineers, which operates dozens of federally owned hydroelectric facilities.

Some two weeks later, the attackers again used Mr. Vitello's account to send a barrage of emails.

One went to Dan Kauffman Excavating Inc., in Lincoln City, Ore., with the subject line: "Please DocuSign Signed Agreement—Funding Project."

HACKING THE GRID
Hack
Attempted hack

Russian hackers
CFE Media
All-Ways Excavating
Corvallis, Ore.-based firm
Commercial Contractors
Dan Kauffman Excavating
Carlson Testing
DeVange Construction
Power companies in New York and Wisconsin
2 Oregon power companies
3 U.K. companies
2 U.S. companies
Massachusetts power company
Sources: documents; interviews with people at the affected companies, government officials and security-industry investigators



Office manager Corinna Sawyer thought the wording was strange and emailed Mr. Vitello: “Just received this from your email, I assume you have been hacked.”

Back came a response from the intruders who controlled Mr. Vitello's account: "I did send it."

Ms. Sawyer, still suspicious, called Mr. Vitello, who told her the email, like the earlier one, was fake.

The attack spreads

One company that got one of the bogus emails was a small professional-services firm in Corvallis, Ore. That July, FBI agents showed up there, telling employees their system had been compromised in a "widespread campaign" targeting energy companies, according to the company owner.

After receiving Mr. Vitello's first bogus email on March 2, a subsequent Homeland Security investigative report says, an employee at the Corvallis firm clicked on the link leading to the hacked voice-over site. She was prompted to enter a username and password. By day's end, the cyberoperatives were in her company's network, according to the report, which hasn't been made public but was reviewed by the Journal.

They then cracked open a portal in the company's firewall, which separates sensitive internal networks from the internet, and created a new account with broad, administrative access, which they hid from view.

"We didn't know about it or catch it," says the company's owner.

Russian hackers
CFE Media
All-Ways Excavating
Corvallis, Ore.-based firm
Commercial Contractors
Dan Kauffman Excavating
Carlson Testing
DeVange Construction
Power companies in New York and Wisconsin
2 Oregon power companies
3 U.K. companies
2 U.S. companies
Massachusetts power company
Sources: documents; interviews with people at the affected companies, government officials and security-industry investigators

In June 2017, the hackers used the Corvallis company's systems to go hunting. Over the next month, they accessed the Oregon company's network dozens of times from

computers with IP addresses registered in countries including Turkey, France and the Netherlands, targeting at least six energy firms.

In some cases, the attackers simply studied the new targets' websites, possibly as reconnaissance for future strikes. In other instances, the investigative report indicates, they may have gained footholds inside their victims' systems.

Two of the targeted companies had helped the Army create independent supplies of electricity for domestic bases.

On June 15, hackers visited the website of ReEnergy Holdings LLC. The renewable-energy company had built a small power plant that allows Fort Drum in western New York to operate even if the civilian power grid collapses. Fort Drum is the home of one of the Army's most frequently deployed divisions and is under consideration to be the site of a $3.6 billion interceptor system to defend the East Coast from intercontinental ballistic missiles.

ReEnergy, owned by private-equity investor Riverstone Holdings LLC, suffered an intrusion but its generating facilities weren't affected, says one person familiar with the matter. The Army was aware of the incident, said a spokesman, who declined to provide additional details.

That same day, the hackers began hitting the website of Atlantic Power[quotes.wsj.com] Corp. , an independent power producer that sells electricity to more than a dozen utilities in eight states and two Canadian provinces. In addition to downloading files from the site, the attackers visited the company's virtual private network login page, or VPN, a gateway to the firm's computer systems for people working remotely, the report says.

Atlantic Power said in a written statement it regularly encounters malicious acts but doesn't comment on specifics. "To our knowledge, there has never been a successful breach of any of the company's systems," it said.

Around midnight that June 28, the hackers used the Corvallis company's network to exchange emails with a 20-person carpentry company in Michigan called DeVange Construction Inc. The emails appeared to come from an employee called Rick Harris—a persona fabricated by the attackers.

DeVange Construction's systems already may have been compromised. Applications to energy companies from nonexistent people seeking industrial-control systems jobs came from DeVange email addresses, according to security experts and emails reviewed by the Journal. Bogus résumés were attached—tweaked to trick recipients' computers into sending login information to hacked servers.

The Journal identified at least three utilities that received the emails: Washington-based Franklin PUD, Wisconsin-based Dairyland Power Cooperative and New York State

Electric & Gas Corp. All three say they were aware of the hacking campaign but don't believe they fell victim to it.

A DeVange employee says federal agents visited the company. The company's owner, Jim Bell, declined to discuss the incident.

That June 30, the hackers sought remote access to an Indiana company that, like ReEnergy, installs equipment to allow government facilities to operate if the civilian grid loses power. That company, Energy Systems Group Ltd. of Newburgh, Ind., a unit of Vectren[quotes.wsj.com] Corp. , declines to say whether it was hacked but says it has a robust focus on cybersecurity.

The company's website says one of its customers is Fort Detrick, an Army base in Maryland with a complex of laboratories that defend the nation against biological weapons. Fort Detrick referred questions to Army officials, who said they take cybersecurity seriously but declined to comment further.

As the summer of 2017 wore on, the attackers took aim at companies that help utilities manage their computer control systems. On July 1, the attackers used the Corvallis company to attack two English companies, Severn Controls Ltd. and Oakmount Control Systems Ltd. Next, they attacked Simkiss Control Systems Ltd. also in England, and accessed "account and control system information," according to the government report.

Simkiss's website says it markets tools that allow technicians to have remote access to industrial control networks. Among its customers are big electrical equipment makers and utilities including National Grid[quotes.wsj.com] , which runs electric transmission lines in Britain and parts of the U.S., where it owns utilities in New York, Rhode Island and Massachusetts.

Oakmount, Severn and Simkiss declined to comment, and National Grid says its cybersecurity processes are "aligned with industry best practice."

After breaching the network of Dan Kauffman Excavating in Oregon, hackers blasted out emails to roughly 2,300 of the company's contacts. PHOTO: LEAH NASH FOR THE WALL STREET JOURNAL

By that fall, the hackers returned to Dan Kauffman Excavating in Oregon, breaching its network on Sept. 18, according to the firm. They appeared to lurk quietly for a month. Then, on the night of Oct. 18, emails blasted out to roughly 2,300 of the company's contacts. The message said, "Hi, Dan used Dropbox to share a folder with you!" and contained a link that said, "View folder."

Among the recipients: employees of PacifiCorp, a multistate utility; the Portland, Ore.-based Bonneville Power Administration, which runs 75% of the Pacific Northwest's high-voltage transmission lines, and the Army Corps of Engineers.

Federal officials say the attackers looked for ways to bridge the divide between the utilities' corporate networks, which are connected to the internet, and their critical-control networks, which are walled off from the web for security purposes.

The bridges sometimes come in the form of "jump boxes," computers that give technicians a way to move between the two systems. If not well defended, these junctions could allow operatives to tunnel under the moat and pop up inside the castle walls.

In briefings to utilities last summer, Jonathan Homer, industrial-control systems cybersecurity chief for Homeland Security, said the Russians had penetrated the control-system area of utilities through poorly protected jump boxes. The attackers had “legitimate access, the same as a technician,” he said in one briefing, and were positioned to take actions that could have temporarily knocked out power.

The federally owned Bonneville Power Administration says it doesn’t believe the utility was breached, though it appears to have received suspicious emails.

PacifiCorp says it takes a multilayered approach to risk management and that it wasn’t compromised by any attack campaigns.

Gary Dodd, Bonneville’s chief information security officer, says he doesn’t believe his utility was breached, though it appears to have received suspicious emails from both All-Ways Excavating and Dan Kauffman Excavating. “It’s possible something got in, but I really don’t think so,” he says.

The Army Corps says it doesn’t comment on cybersecurity matters.

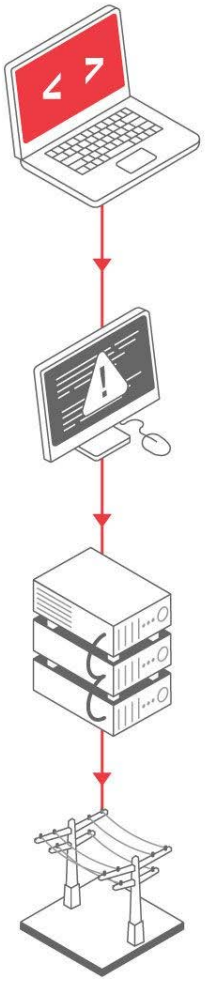
Going public

The U.S. government warned the public about the hacking campaign in an October 2017 advisory. It attributed it to a shadowy group, sometimes called Dragonfly or Energetic Bear, that security researchers have tied to the Russian government.

In March 2018, the U.S. went further, releasing a report that pinned responsibility for the hostile activities on “cyber actors” working for the Russian government, saying they had been active since at least March 2016. Governments generally have shied away from naming countries involved in cyberattacks, not wanting divulge what they know.

Short Circuit

Russian hackers targeted utilities' control-system computers.



Russian hackers use malicious emails to steal credentials from utility company employees.
Employee computer
Using stolen credentials, hackers remotely access power-utility workstations and run malicious code.
Scada server
From the compromised workstation, hackers can gain access to the utility’s supervisory control and data acquisition system (Scada).
Electrical equipment
Scada controls utility assets, including substations and power-generation facilities.

Sources: Department of Homeland Security (hacking); Department of Energy (Scada network)

In April 2018, the FBI notified at least two companies by letter that they appeared to have received malicious emails from All-Ways Excavating's Mr. Vitello.

One was Commercial Contractors of Ridgefield, Wash., which helped renovate an office for the Bonneville Power Administration. Eric Money, the company's president, says employees thought they had resisted the tainted emails. But the Journal found that a computer with an IP address linked to the company visited Mr. Hudson's hacked voice-over site the day of the attack.

The other company notified by the FBI, Carlson Testing of Tigard, Ore., has done work for utilities including Portland General Electric, PacifiCorp, Northwest Natural Gas and the Bonneville Power Administration.

Vikram Thakur, technical director of security response for Symantec[quotes.wsj.com] Corp. , a California-based cybersecurity firm, says his company knows from its utility clients and from other security firms it works with that at least 60 utilities were targeted, including some outside the U.S. About two dozen were breached, he says, adding that hackers penetrated far enough to reach the industrial-control systems at eight or more utilities. He declined to name them.

The government isn't sure how many utilities and vendors in all were compromised in the Russian assault.

Vello Koiv, president of VAK Construction Engineering Services in Beaverton, Ore., which does subcontracting for the Army Corps, PacifiCorp, Bonneville and Avista[quotes.wsj.com] Corp. , a utility in Spokane, Wash., says someone at his company took the bait from one of the tainted emails, but his computer technicians caught the problem, so "it was never a full-blown event." Avista says it doesn't comment on cyberattacks.

Mr. Koiv says he continued to get tainted emails in 2018. "Whether they're Russian or not, I don't know. But someone is still trying to infiltrate our server."

Last fall, All-Ways Excavating was again hacked.

Industry experts say Russian government hackers likely remain inside some systems, undetected and awaiting further orders.

Write to Rebecca Smith at rebecca.smith@wsj.com and Rob Barry at rob.barry@wsj.com

Appeared in the January 11, 2019, print edition as 'Russian Hack Exposes Weakness in U.S. Power Grid.'

THE TRUE COST OF COMPLIANCE WITH DATA PROTECTION REGULATIONS

BENCHMARK STUDY OF MULTINATIONAL ORGANIZATIONS

Sponsored by Globalscape
Independently conducted by Ponemon Institute LLC
Publication Date: December 2017

GLOBALSCAPE

Ponemon INSTITUTE

CONTENTS

PART 1

EXECUTIVE SUMMARY

Multinational organizations in all industries must comply with privacy and data protection laws, regulations and policies designed to protect individuals' sensitive and confidential information. Compliance requires organizations to adopt and implement a variety of costly activities that include process, people and technologies. In this year's study, companies expressed concern about achieving compliance with the EU's General Data Protection Regulation (GDPR) by May 25, 2018.

> The key takeaway from this study is that it pays to invest in compliance. Specifically, if companies spent more on compliance activities such as audits, enabling technologies, training and expert staffing, it would be less costly than if they were in non-compliance with data protection regulations.

Ponemon Institute and Globalscape conducted The True Cost of Compliance with Data Protection Regulations to determine the full economic impact of compliance activities for a representative sample of 53 multinational organizations. An earlier study was completed in 2011 and those findings are compared to this year's results.[1]

The objective of this research is to determine the full costs associated with an organization's compliance efforts, including the cost of non-compliance with laws, regulations and policies. In order to be as accurate as possible in our cost estimates, we interviewed 237 individuals involved in compliance activities in benchmarked organizations.

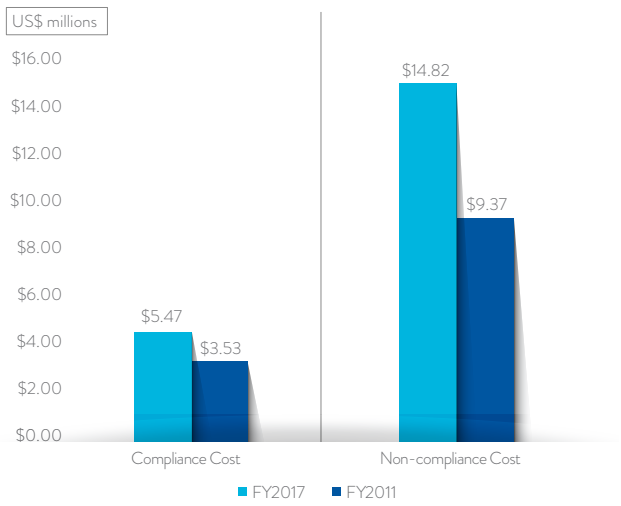
COMPANIES ARE SPENDING MORE ON COMPLIANCE AND THE CONSEQUENCES OF NON-COMPLIANCE

As shown in Figure 1, while the average cost of compliance for the organizations in our current study is $5.47 million, a 43 percent increase from 2011, the cost of not being in compliance is much greater.[2]

The average cost for organizations that experience non-compliance problems is $14.82 million, a 45 percent increase from 2011.

Thus, investing in the compliance activities described in this study can be beneficial in avoiding such non-compliance problems as business disruption, declines in productivity, fees, penalties and other legal and non-legal settlement costs.

Figure 1. Difference between Compliance and Non-compliance Cost



THE COST OF BEING IN COMPLIANCE

Companies invest in compliance activities because of laws and regulations and not necessarily to improve their security posture. Regulations that are a priority are the EU's General Data Protection Regulation (GDPR), PCI DSS, HIPAA and various state privacy and data protection laws, country-specific laws and Sarbanes-Oxley.

In the course of our research, we learned that many organizations face multiple and sometimes competing compliance challenges that require constant monitoring and frequent audits. As a result, compliance can be a significant cost burden that includes the need to have dedicated professional staff, enabling technologies to curtail risk and allocation of legal and non-legal penalties for non-compliance.

Following are typical compliance costs:

- Data protection and enforcement activities
- Incident response plans
- Compliance audits and assessments
- Policy development
- Communications & training
- Staff certification
- Redress activities
- Investments in specialized technologies to protect data assets such as threat intelligence, managed file transfer, identity and access governance, cyber analytics, data loss prevention, encryption and more

THE COST OF NON-COMPLIANCE

Non-compliance costs are those that result when a company fails to comply with rules, regulations, policies, contracts and other legal obligations. Following are costs due to non-compliance.

These costs, as shown in this report, are 2.71 times the cost of compliance:

- Business disruption
- Productivity losses
- Revenue losses
- Fines, penalties and settlement costs

INDUSTRY AND ORGANIZATIONAL SIZE AFFECT THE COST OF COMPLIANCE AND NON-COMPLIANCE

Understandably, organizations in heavily regulated industries such as financial services and healthcare have the highest compliance costs. Such costs are also affected by the amount of sensitive and confidential information an organization must secure.

The cost of compliance varies significantly by the organization's industry sector, ranging from $7.7 million for media to more than $30.9 million for financial services.

The percentage net increase in total compliance cost between 2011 and 2017 also varies by industry. Healthcare organizations and technology and software organizations experienced the highest growth in cost at 106 percent and 99 percent, respectively. Energy, utilities and retail companies show the lowest growth in total compliance cost at 6 percent and 40 percent, respectively, between 2011 and 2017.

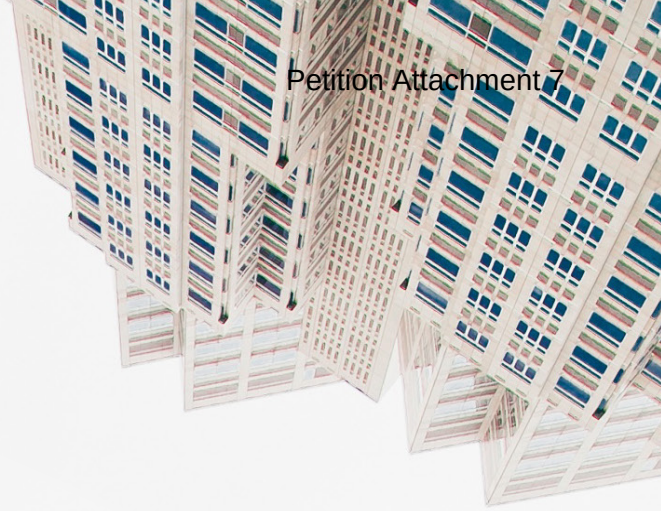
When adjusting compliance and non-compliance costs by each organization's headcount, smaller-sized companies (less than 5,001 employees) incur substantially higher per-capita compliance costs than larger companies (more than 5,000 employees).

THE FOLLOWING FACTORS LOWER THE TOTAL COST OF COMPLIANCE

The more effective an organization's security posture is, the lower the cost of non-compliance. Using a well-known indexing method that measures each organization's security posture, called the security effectiveness score (SES), we determined that security effectiveness is unrelated to compliance cost. However, SES appears to be inversely related to non-compliance cost. Thus, organizations with a higher score (more favorable security posture) experience a lower cost of non-compliance.

Corporate investment in compliance reduces the negative consequences and cost of non-compliance. Per capita non-compliance cost is inversely related to the percentage of compliance spending in relation to the total IT budget. Clearly, a higher percentage for compliance spending relative to the total IT budget is an indication that corporate investment in compliance reduces the negative consequences and cost of non-compliance.

Ongoing compliance audits reduce the total costs of compliance. Per capita non-compliance cost appears to be inversely related to the frequency of compliance audits, whereas organizations that do not conduct compliance audits experience the highest compliance cost when adjusted for size.



PART 2
KEY FINDINGS

In this section, we provide a deeper analysis of what affects the cost of compliance and non-compliance and why non-compliance costs are significantly higher. The report is organized according to the following topics:

- The cost of compliance
- The cost of non-compliance
- The impact of governance and regulations on the cost of compliance
- The impact of security posture on the cost of compliance

The key findings presented below are based on the benchmark analysis of 53 multinational organizations located in the United States. We obtained information about each organization's data compliance cost utilizing an activity-based costing method and a proprietary diagnostic interviewing technique involving 237 functional leaders. Our research methods captured information about direct and indirect costs associated with compliance activities during a 12-month period. We define a compliance activity as one that organizations use to meet the specific rules, regulations, standards, policies and contracts that are intended to protect information assets.

Our benchmarking efforts also captured the direct, indirect and opportunity costs associated with non-compliance events during a 12-month period. We define non-compliance cost as the cost that results when a company fails to comply with rules, regulations, policies, contracts, and other legal obligations. The Appendix of this report discusses our benchmarking methods in greater detail.

In the course of interviewing functional leaders, we determined key trends and commonalities between both compliance and non-compliance costs. For many organizations, compliance has a very broad scope that includes global privacy, financial data integrity, data loss notification, credit cardholder protection, and other regulatory mandates. It also includes self-regulatory frameworks including ISO, NIST and others.

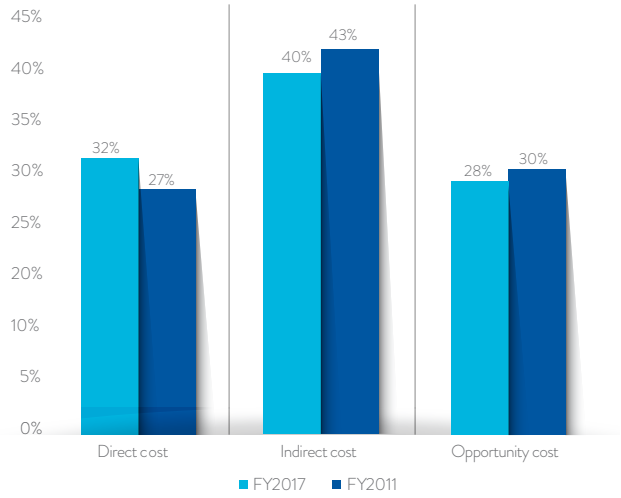
THE COST OF COMPLIANCE

Organizations spend the most on administering their compliance programs. Figure 2 reports how costs are allocated on a percentage basis for all data compliance cost activities combined.

As shown, indirect costs, such as administrative overhead, account for 40 percent of compliance cost activities. Direct costs such as payments to consultants, auditors or other outside experts represents 32 percent, which increased by five percent between 2011 and 2017. Opportunity costs, such as an organization's inability to execute a marketing campaign because of consumer privacy concerns, represent 28 percent.

Data security has the highest costs with policy representing the lowest costs; the average cost of data security is $2 million.

Figure 2. Percentage cost structure for compliance costs
Computed from 53 benchmarked companies



As discussed previously, the cost of compliance can range from $5.5 million to almost $22 million. Table 1 summarizes the total, average, median, maximum and minimum compliance costs for each of the six activity centers defined in our cost framework in Part 5. Please note that these cost statistics are defined for a 12-month period. Data security represents the largest cost center, while policy represents the smallest center of cost activities for the benchmark sample.

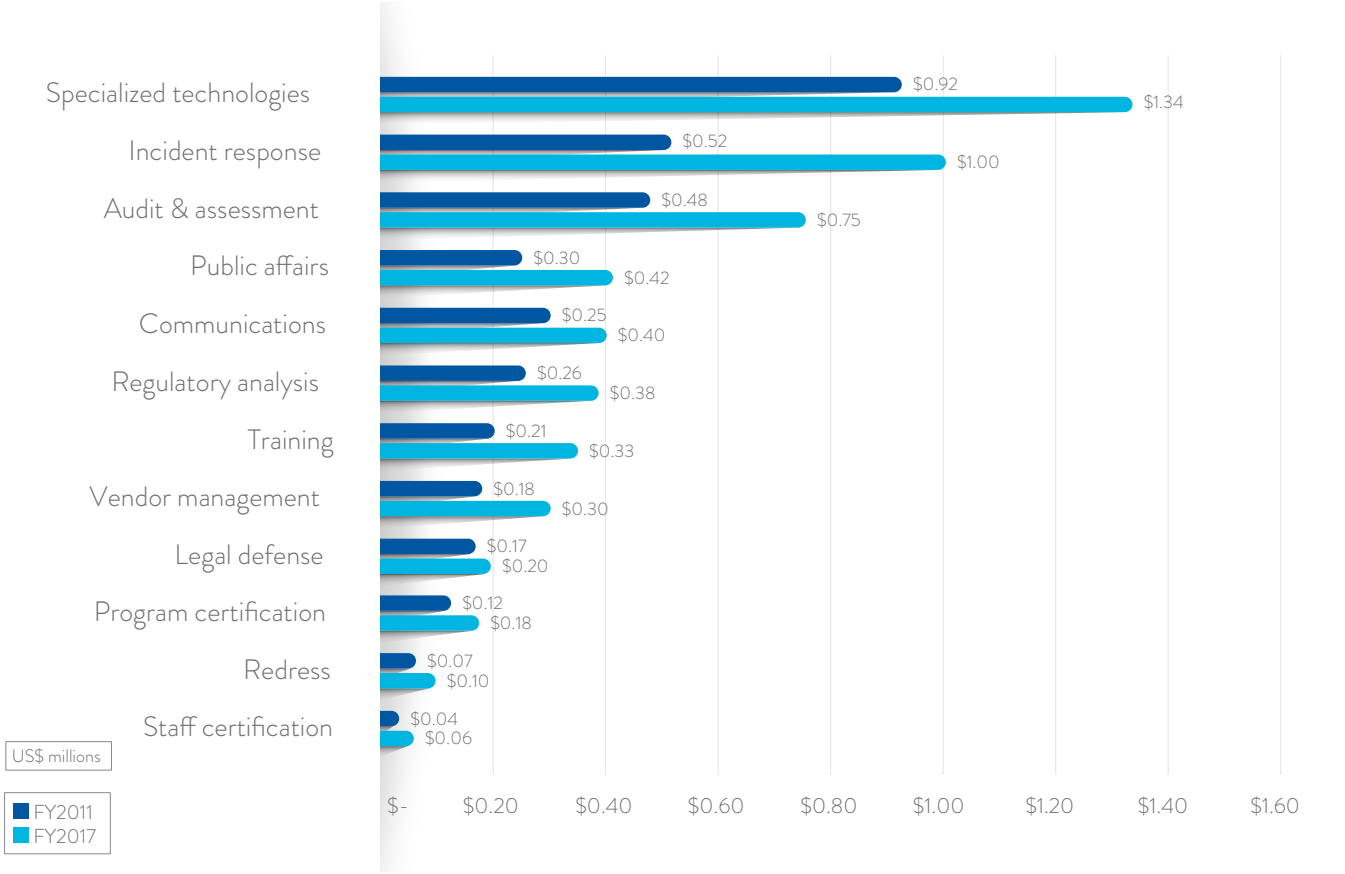
Table 1. Key statistics on the cost of compliance for six activity centers

Activity centers	Average	Median	Maximum	Minimum
Policy	$399,601	$296,032	$583,421	$0
Communications & training	$378,590	$289,669	$1,711,992	$45,600
Program management	$673,010	$530,219	$3,305,664	$89,104
Data security*	$2,010,800	$1,359,257	$6,592,051	$287,556
Forensics & monitoring	$1,089,455	$832,145	$6,241,897	$356,212
Enforcement	$917,703	$663,839	$7,126,414	$106,000
Overall	$5,469,159	$3,971,161	$21,561,439	$1,431,425

**Sixty-five percent of this center pertains to the direct and indirect costs associated with enabling security technologies.*

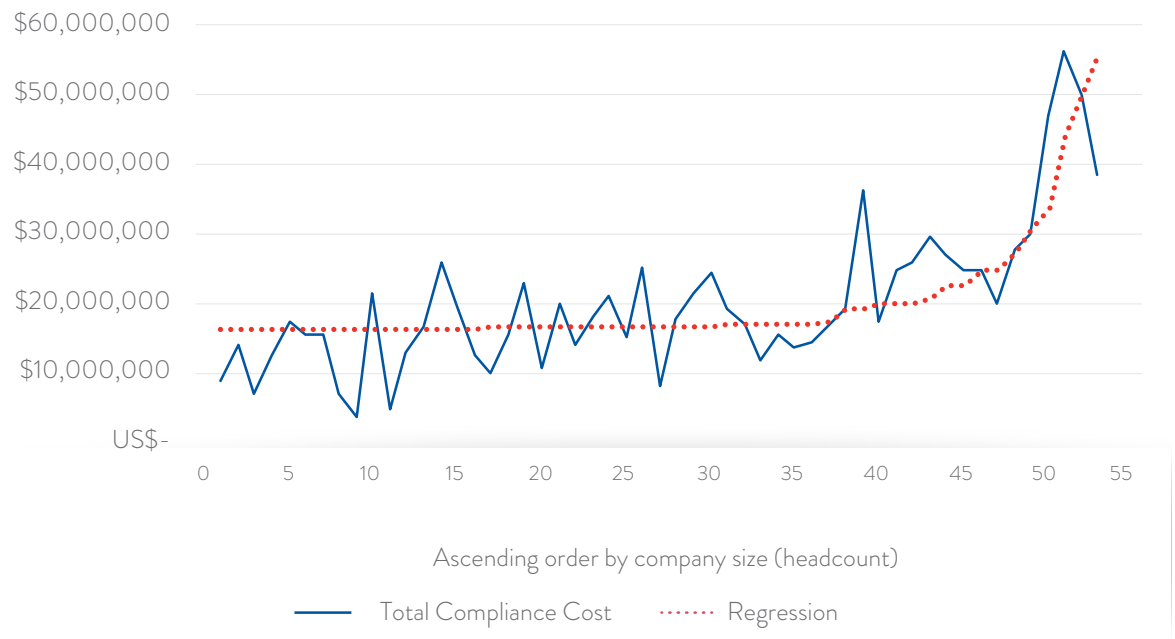
Companies invest most in compliance-related technologies and incident response. The following two figures show the average compliance cost activities for 53 organizations. As shown in Figure 3, compliance costs relating to compliance technologies and incident response represent the two largest expenditure categories. This chart also shows an increase in the amount spent on all expense categories. Between 2011 and 2017, the amount spent on technologies increased by 36 percent, and the amount spent on incident response increased by 64 percent.

Figure 3. Compliance costs by expense categories
Computed from 53 benchmarked companies



Organizational size affects total compliance costs. Figure 4 shows total compliance cost, which is the combination of compliance cost and non-compliance cost, for 53 benchmarked organizations. The chart and regression line reveals a strong linear relationship between size and cost.

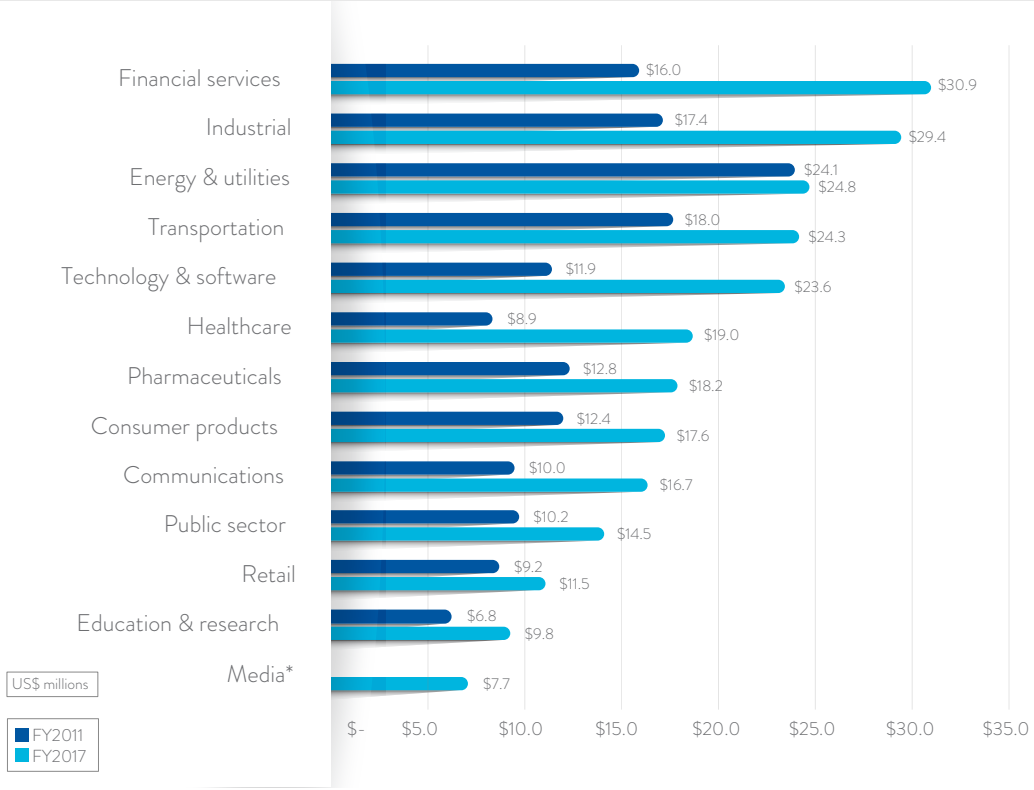
Figure 4. Total compliance cost by organizational headcount (size)
Computed from 53 benchmarked companies



Compliance costs increase the most for financial services and industrial companies. Figure 5 provides total compliance cost for 13 industries in our benchmark sample. The analysis by industry is limited because of a small sample size; however, it is interesting to see wide variation across segments, ranging from a high of $30.9 million in financial services to a low of $7.7 million for media companies. It is also important to note that total compliance cost for each industry segment increased between 2011 and 2017.

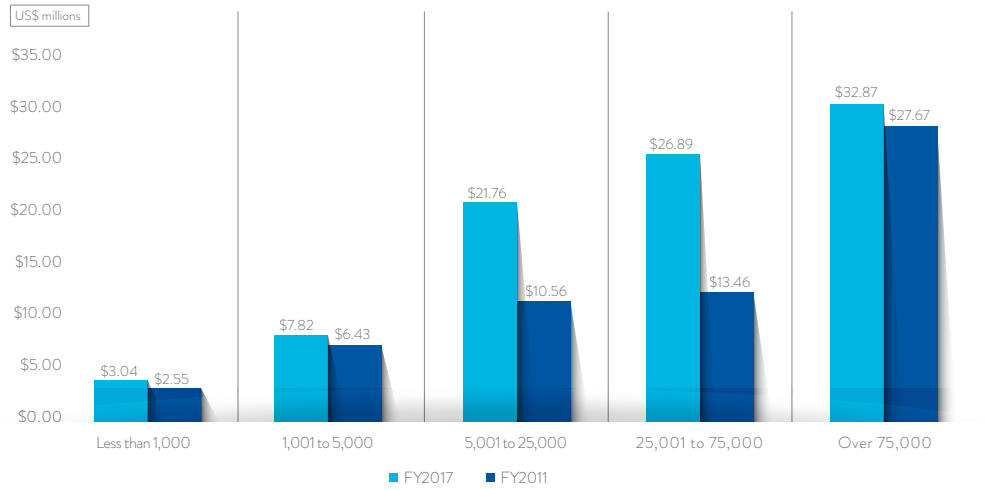
Figure 5. Total compliance cost by industry

*Computed from 53 benchmarked companies | *2011 data is not available*



Larger companies have higher compliance costs. Figure 6 reports the average total compliance costs by the approximate global headcount (size) of benchmark companies. As seen here, total compliance costs increase by organizational size in 2011 and 2017.

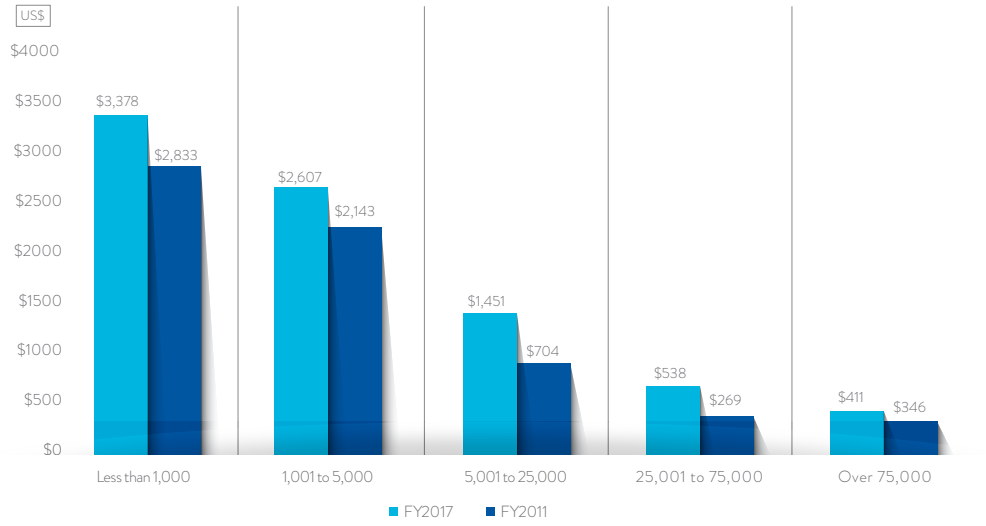
Figure 6. Total compliance cost by headcount
Computed from 53 benchmarked companies



Smaller organizations have higher per capita costs of compliance. Figure 7 provides an analysis of total compliance cost on a per capita basis. When adjusted by headcount (size), compliance costs are highest for organizations with fewer than 1,000 employees and smallest for organizations with 75,000 or more employees.

This result may be explained in part by economy of scale, wherein larger companies have access to leading data protection technologies and highly skilled personnel who have expertise in data protection laws and regulations. Organizations with fewer than 5,000 employees have to rely on expensive external resources such as consultants and lawyers to meet compliance requirements on a global scale.

Figure 7. Per capita total compliance cost by global headcount (size)
Computed from 53 benchmarked companies



THE COST OF NON-COMPLIANCE

Business disruption and productivity loss are the highest costs for non-compliance. Table 2 summarizes the total, average, median, maximum and minimum non-compliance cost for each one of four consequences defined in our framework for a 12-month period. Business disruption represents the most costly consequence, while fines, penalties and other settlement costs represent the least costly consequences of compliance failure.

Table 2. Key statistics on the cost of non-compliance for four activity centers

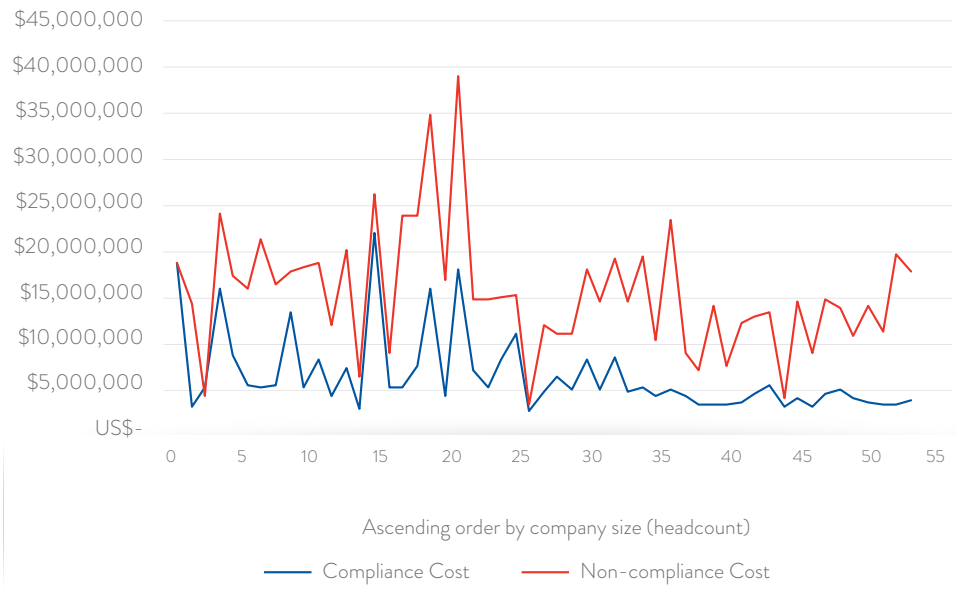
Non-compliance cost consequences	Average	Median	Maximum	Minimum
Business disruption	$5,107,206	$4,232,786	$20,396,716	$1,100,745
Productivity loss	$3,755,401	$4,667,300	$17,336,500	$997,600
Revenue loss	$4,005,116	$3,995,194	$19,176,931	$ –
Fines, penalties & other	$1,955,674	$1,100,500	$5,301,500	$ –
Overall	$14,823,397	$13,995,780	$39,223,575	$2,200,868

Companies are not spending enough on core compliance activities. Figure 8 shows compliance, non-compliance and total compliance costs for 54 organizations. The range for compliance cost is $0.58 million to $21.56 million. The range for non-compliance cost is $2.20 million to $39.22 million. As seen here, in all but two cases, non-compliance costs exceeded compliance costs.

The gap between compliance and non-compliance provides evidence that organizations do not spend enough resources on core compliance activities. In other words, if companies spent more on compliance such as audits, enabling technologies, training, expert staffing and more, they would experience a more than commensurate reduction in non-compliance cost.

Figure 8. Compliance and non-compliance costs

Computed from 53 benchmarked companies



COMPLIANCE SPENDING AND BUDGET

Figure 9 reports the percentage of compliance spending with respect to the organization's total IT budget. The extrapolated average percentage in 2011 is 11.8 percent. In 2017, the extrapolated average percentage is 14.3 percent.

Figure 9. Percentage of compliance spending to the total IT budget
Computed from 53 benchmarked organizations

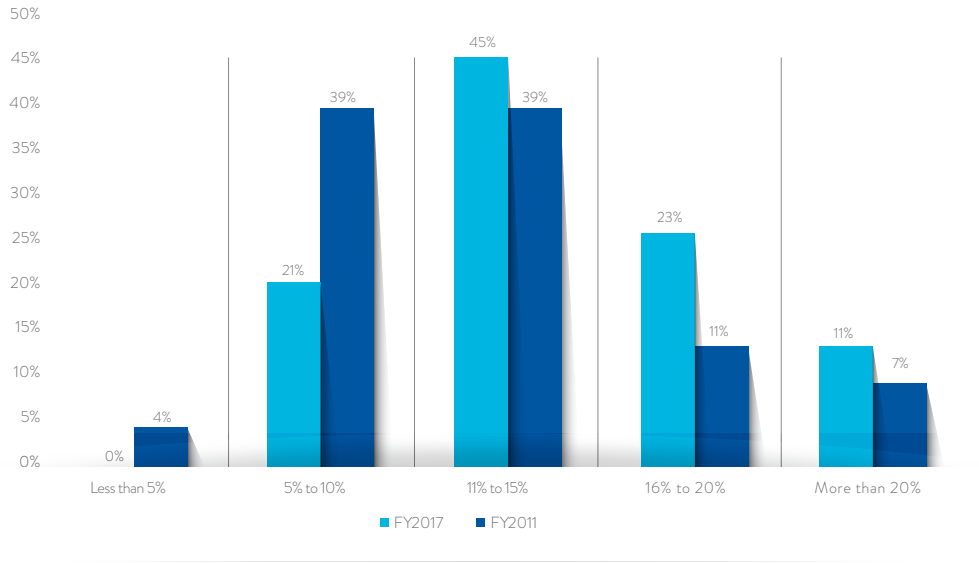
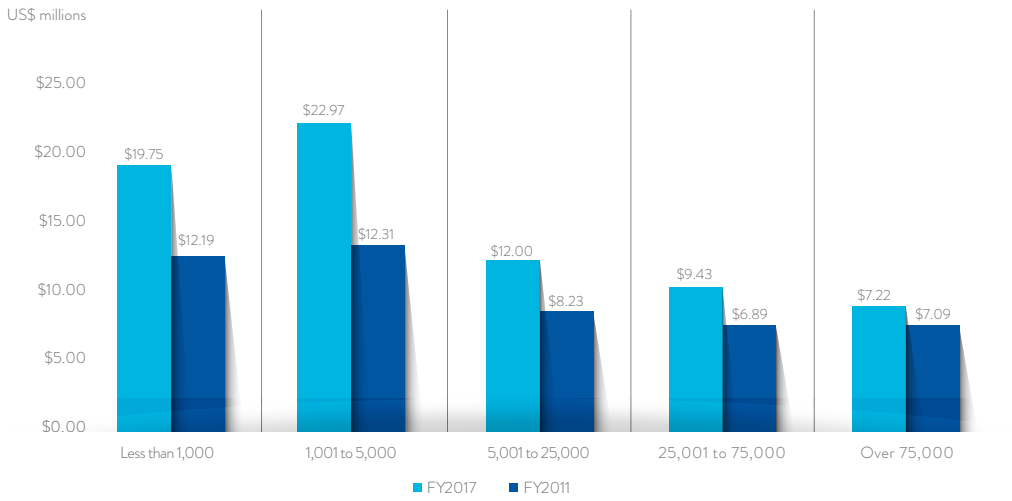


Figure 10 reveals another interesting relationship between compliance spending and non-compliance cost. As shown, non-compliance cost is inversely related to the percentage of compliance spending.

Figure 10. Non-compliance cost by percentage of the IT budget
Computed from 53 benchmarked organizations

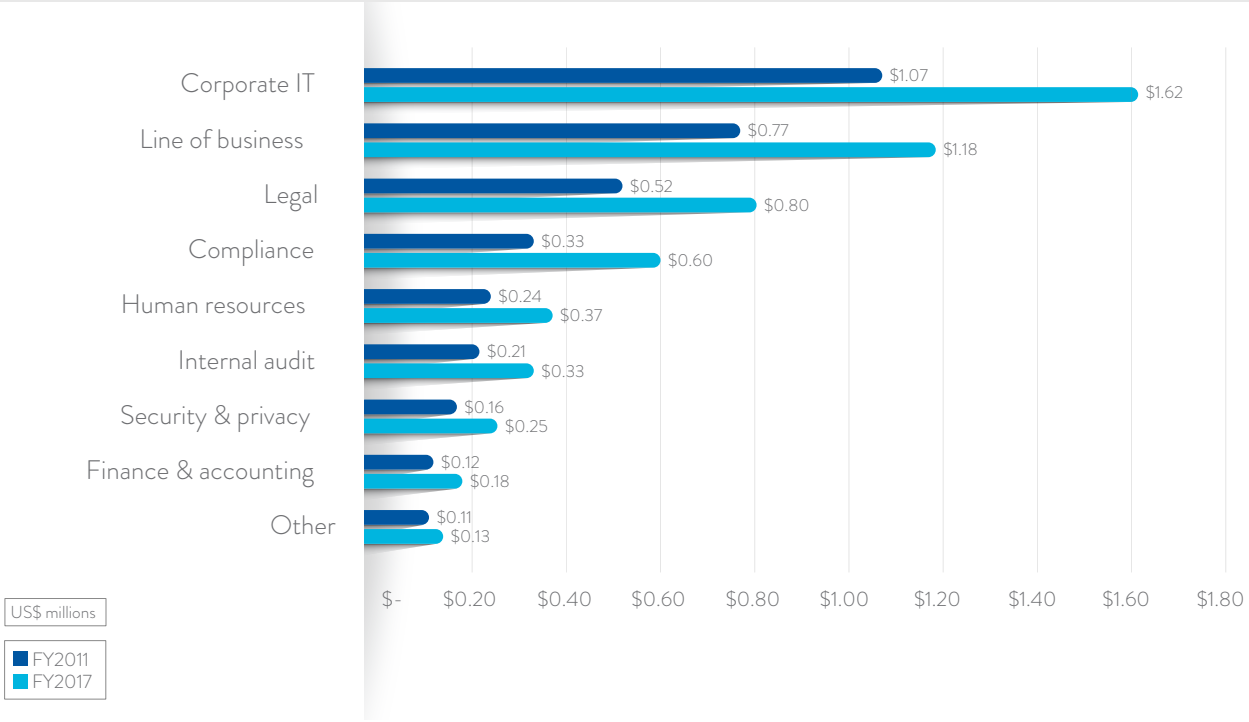


THE IMPACT OF GOVERNANCE AND REGULATIONS ON THE TOTAL COST OF COMPLIANCE

Corporate IT, lines of business and legal are most likely to own or influence compliance expenditures relating to data protection and privacy, as shown in Figure 11. It also shows all functions increasing the amount spent on compliance. Here, corporate IT and line of business experienced the highest net increase between 2011 and 2017, at 40 percent and 42 percent, respectively.

Figure 11. Compliance costs by functional area

Computed from 53 benchmarked companies

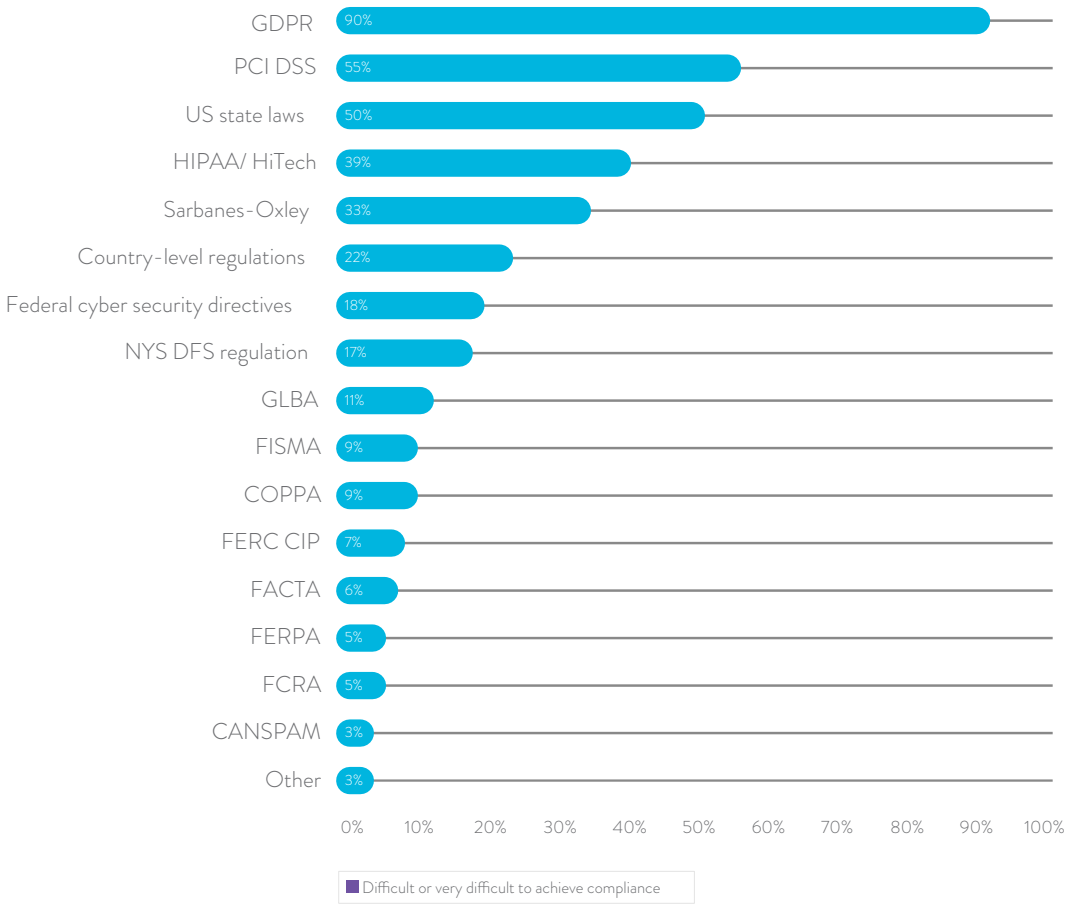


Compliance with GDPR is considered difficult to achieve. This analysis concerns how 237 respondents in our sample of 53 benchmarked organizations view different data compliance regulations in terms of importance and difficulty. Clearly, certain regulations are specified by industry (such as HIPAA, GLBA, FISMA).

PCI DSS, various US state data breach or privacy laws, Sarbanes-Oxley and country-level regulations are also viewed as difficult or very difficult to meet compliance requirements.

Figure 12 shows that 90 percent of respondents view GDPR compliance as the most difficult to achieve.

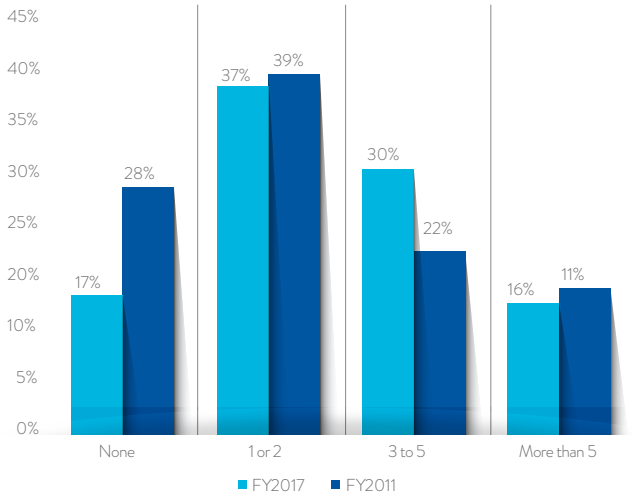
Figure 12. Regulatory compliance requirements difficult to achieve
Computed from 53 benchmarked organizations



MOST COMPANIES CONDUCT ONE OR MORE COMPLIANCE AUDITS ANNUALLY

Figure 13 reports the annual internal compliance audit frequency of participating benchmark companies.[3] The pattern of response for 2011 and 2017 is generally consistent. In 2011, a total of 72 percent (100%-28%) of companies said they conduct data compliance audits one or more times each year (or an average of 2.2 audits). In 2017, a total of 83 percent (100%-17%) of companies said they perform data compliance audits each year (or an average of 2.9 audits).

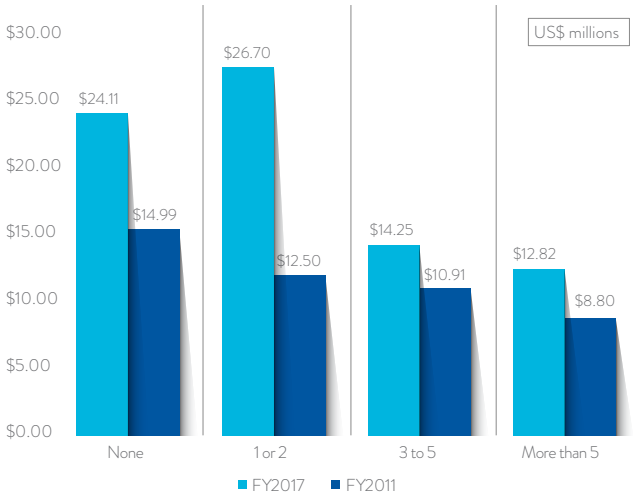
Figure 13. Internal audit frequency
Computed from 53 benchmarked organizations



MORE COMPLIANCE AUDITS REDUCE THE COST OF COMPLIANCE

Figure 14 shows the inverse relationship between total compliance cost and internal audit frequency. As can be seen, organizations that conduct five or more internal compliance audits per year have the lowest total compliance cost in both 2011 and 2017. The highest total compliance cost in the current study ($26.7 million) pertains to organizations that conduct one or two internal compliance audits per year.

Figure 14. Total compliance cost by audit frequency
Computed from 53 benchmarked organizations



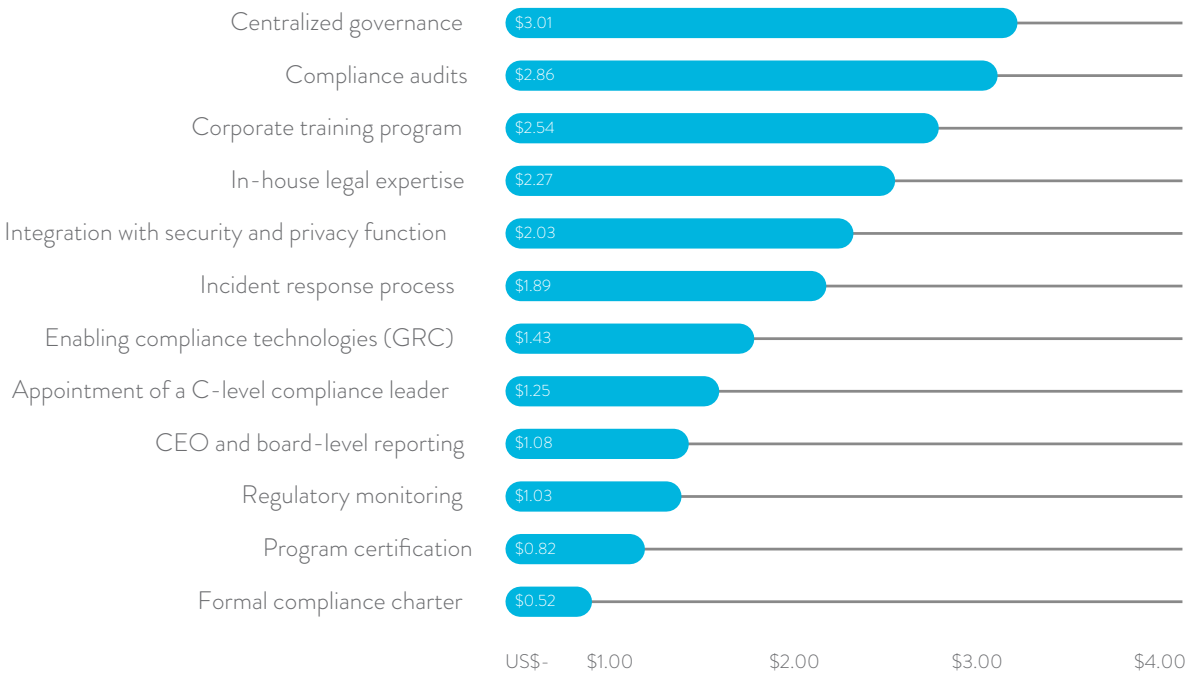
CENTRALIZED GOVERNANCE AND AUDITS REDUCE TOTAL COMPLIANCE COSTS

Figure 15 summarizes the incremental cost savings resulting from the implementation of 12 best practices.

For example, the deployment of a centralized data governance program reduces total compliance cost by $3.01 million. Similarly, conducting compliance audits reduces total compliance costs by $2.86 million. Other best practices that are cost saving include corporate training programs, in-house legal experts, integration of security and privacy functions and a fully functional incident response process.

Figure 15. Twelve best practices that reduce total compliance costs

Computed from 53 benchmarked organizations



THE IMPACT OF SECURITY POSTURE ON THE COST OF COMPLIANCE

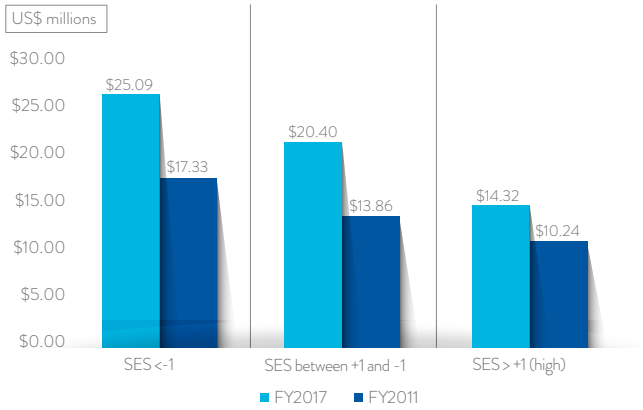
In this benchmark study, we utilize an indexing methodology known as the Security Effectiveness Score (SES) to measure an organization's ability to meet reasonable security objectives.[4] Recent research shows that the higher the SES index, the more effective the organization is in protecting information assets and critical infrastructure.

The SES range of possible scores is -2 (minimum score) to +2 (maximum score). Index results for the present benchmark sample vary from a low of -1.60 to a high of +1.73, with a mean value at +.21. In the 2011 study, the lowest score was -1.67, the highest score was +1.69 and the mean SES was +.18.

As with prior Ponemon Institute research, we measured the security posture of participating organizations as part of the benchmarking process for this study. Figure 16 reports the total compliance cost in ascending order by SES. This graph clearly shows an inverse relationship between effectiveness score and compliance cost. Specifically, companies with an SES above +1 have the lowest total compliance cost. Companies with an SES below -1 have the highest total compliance cost.

Figure 16. Benchmark sample in ascending order by SES

Computed from 53 benchmarked companies

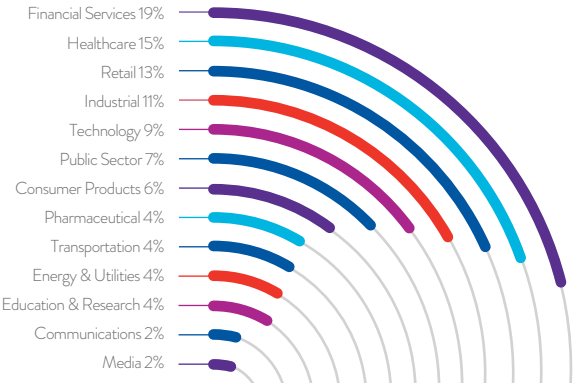


PART 3

SAMPLE OF PARTICIPATING ORGANIZATIONS

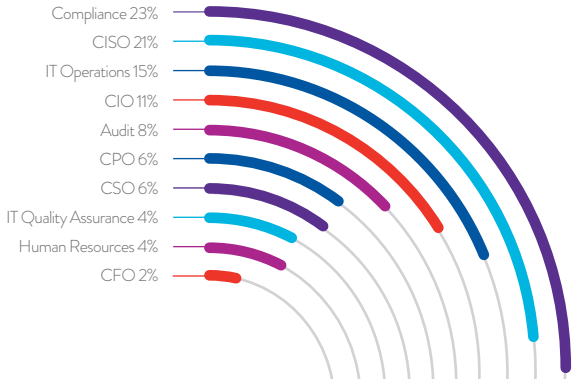
Pie Chart 1. Industry classification of the benchmark sample
Computed from 53 benchmarked companies

Pie Chart 1 reports the percentage of companies by industry that participated in the benchmark study. Our final sample includes a total of 53 organizations, which serves as the unit of analysis. As previously mentioned, a total of two organizations were rejected from the final sample for incomplete responses to interview questions or survey responses. As shown, financial services, healthcare and retail organizations represent the three largest segments.



Pie Chart 2. Participating respondents by their approximate job function or title

Computed from 237 separate interviews



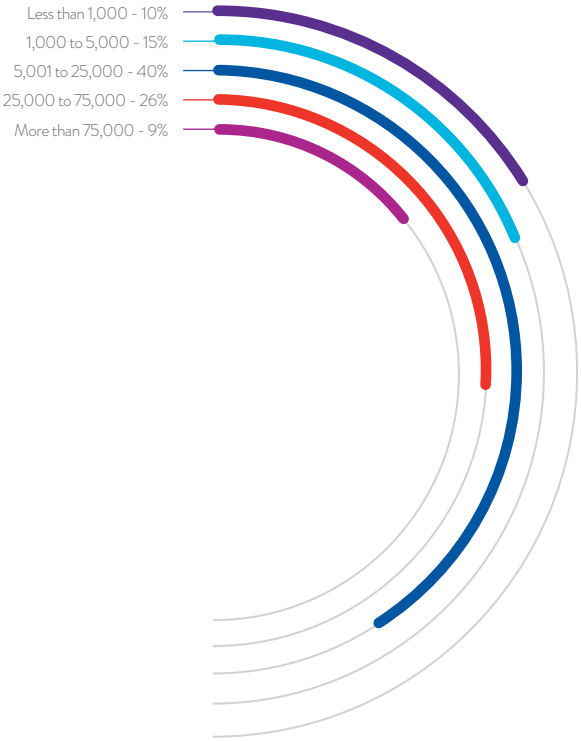
Pie Chart 2 reports the approximate job functions or titles of participants who completed the diagnostic interview. In total, 237 individuals with responsibility for data protection compliance activities were engaged in the benchmark research process.

Pie Chart 3. Distribution of participating organizations by global headcount

Computed from 53 benchmarked companies

On average, benchmark methods required four or five interviews to capture enough information to extrapolate compliance and non-compliance costs. As seen in Pie Chart 1, respondents in information security, compliance, and IT operations represent the top three functional areas participating in these diagnostic interviews.

Pie Chart 3 summarizes the global headcount of participating organizations, wherein the largest segment includes organizations with 5,001 to 25,000 full-time equivalent employees. Accordingly, headcount is used as a surrogate for organizational size in this research.



PART 4

CONCLUSION

To reduce the total cost of compliance and offset the risk of non-compliance, security strategies should integrate enabling technologies with people, policies and operational processes. The following 16 attributes have the strongest correlation to creating an effective security posture while meeting data compliance goals of an organization. These attributions from the security effectiveness score (SES) instrument have the highest negative correlation to non-compliance cost as compiled from 53 benchmark companies. This means that these attributes are most supportive of a strong compliance culture.

- Monitor and strictly enforce security policies
- Conduct audits or assessments on an ongoing basis
- Attract and retain highly skilled security personnel
- Provide company-wide training and awareness activities
- Minimize downtime or disruptions to business processes
- Prevent or curtail malware or non-malware attacks
- Measure the effectiveness of the data security program
- Ensure security program is consistently managed
- Know where sensitive or confidential information resides
- Secure all endpoints to the network (including IoT devices)
- Implement strong identity and authentication processes
- Reduce data clutter, especially unstructured data assets
- Develop a data compliance governance strategy
- Develop a communication channel to the CEO and board
- Obtain C-level support for data compliance and privacy
- Create and test an incident response process

Essential to achieving substantial compliance goals requires holistic and integrated security solutions that ensure every aspect of the organization is covered and protection works seamlessly. Recent benchmark research conducted by Ponemon Institute provides insights from information security leaders on how to build an integrated and holistic security strategy.

Today's security challenges require organizations to anticipate how changing threats will affect their organization's ability to comply with external, internal and contractual demands. We have identified four primary security challenges that affect all organizations. They are: external and internal threats to security, the changing workforce, changing business models and processes and the changing world. Understanding the implications of these security challenges will help organizations succeed in aligning their core practices and technologies across the enterprise in ways that minimize the risk of compliance failure. Following are security challenges and how to respond to them:

- External and internal security threats
  Changing threats requires an organization to do the following: make security an integral part of its culture; keep pace with technological advances; "design-in" security in business processes to "design-out" compliance risks; understand the latest threats and actively assess the insider threat.
- The changing workforce
  Changing workforce requires organizations to: make sure security keeps pace with organizational restructuring and change; audit, grant or withdraw access rights to property and systems; have adequate screening procedures for new employees and determine whether remote workers are securely accessing the network.
- Changing business models and processes
  Business changes require organizations to secure business processes during periods of transition; understand operational dependencies; verify that business partners have sufficient security practices in place; secure the transfer of information assets between different organizations; and review, audit and, when necessary, revoke access rights.
- Change the world
  Finally, a quickly changing environment requires organizations to have the technologies and plans in place to deal with attacks upon the critical infrastructure, theft of information assets and other criminal incidents.

What are the implications for an organization that does not have the right integrated and holistic response to data security and related compliance challenges? The consequence of not managing compliance risks include a loss of trust that will jeopardize customer loyalty, and the inability to deliver services and products causing revenues to decline.

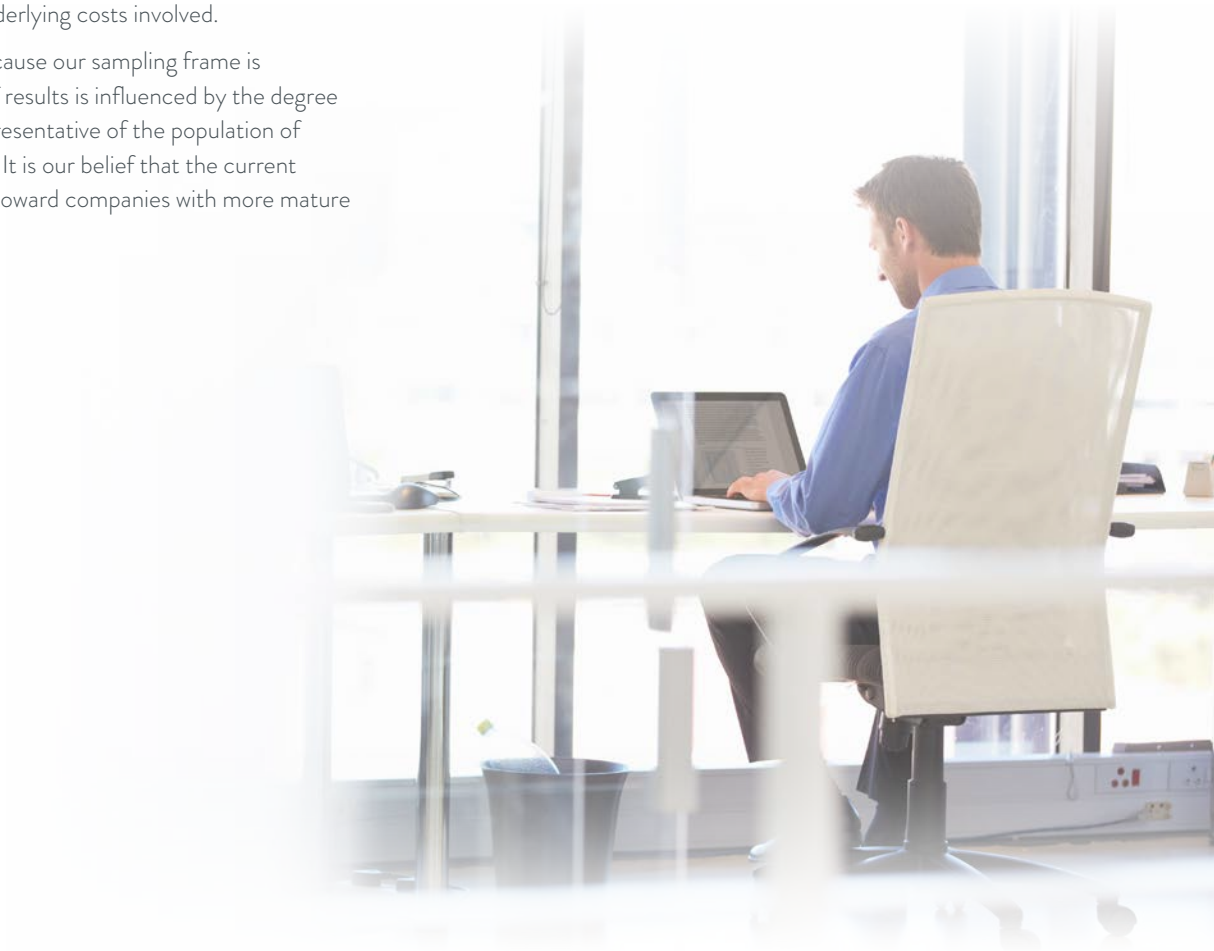
Beyond the economic impact, non-compliance increases the risk of losing valuable information assets such as intellectual property, physical property and customer data. Further, non-compliant organizations risk becoming victims of cyber fraud, business disruption, and many other dangers that might cause them to fail.

We believe our study demonstrates that an investment in both external and internal compliance activities is beneficial not only to the security but also to the overall operations of an organization. By investing in compliance activities, we have shown that organizations reduce the risk created by non-compliance. By considering the above practices, organizations can enjoy better compliance for a given level of investment. Further, the results of this study will help corporate IT and lines of business demonstrate the value of investing in their compliance activities.

CAVEATS

This study utilizes a confidential and proprietary benchmark method that has been successfully deployed in earlier Ponemon Institute research. However, there are inherent limitations to benchmark research that need to be carefully considered before drawing conclusions from findings.

- Non-statistical results: The purpose of this study is descriptive rather than normative inference. The current study draws upon a representative, non-statistical sample of data centers, all located in the United States. Statistical inferences, margins of error and confidence intervals cannot be applied to these data given the nature of our sampling plan.
- Non-response: The current findings are based on a small representative sample of completed case studies. An initial mailing of benchmark surveys was sent to a reference group of over 200 separate organizations. Fifty-three organizations provided usable benchmark surveys. Non-response bias was not tested so it is always possible companies that did not participate are substantially different in terms of the methods used to manage the detection, containment and recovery process, as well as the underlying costs involved.
- Sampling-frame bias: Because our sampling frame is judgmental, the quality of results is influenced by the degree to which the frame is representative of the population of companies being studied. It is our belief that the current sampling frame is biased toward companies with more mature compliance programs.
- Company-specific information: The benchmark information is sensitive and confidential. Thus, the current instrument does not capture company-identifying information. It also allows individuals to use categorical response variables to disclose demographic information about the company and industry category. Industry classification relies on self-reported results.
- Unmeasured factors: To keep the survey concise and focused, we decided to omit other important variables from our analyses such as leading trends and organizational characteristics. The extent to which omitted variables might explain benchmark results cannot be estimated at this time.
- Estimated cost results: The quality of survey research is based on the integrity of confidential responses received from benchmarked organizations. While certain checks and balances can be incorporated into the data capture process, there is always the possibility that respondents did not provide truthful responses. In addition, the use of a cost estimation technique (termed shadow costing methods) rather than actual cost data could create significant bias in presented results.



PART 5
COST FRAMEWORK

Our primary method for determining the total cost of compliance relies on the objective collection of cost data. Using a well-known cost accounting method, we were able to allocate detailed cost data into discernible activity centers that explain the entire data protection and compliance mandate within benchmarked companies.[5] We determined that the following six cost activity centers explain the full economic impact of compliance costs associated with data protection. Within each center, we compile the direct and indirect costs associated with each activity.

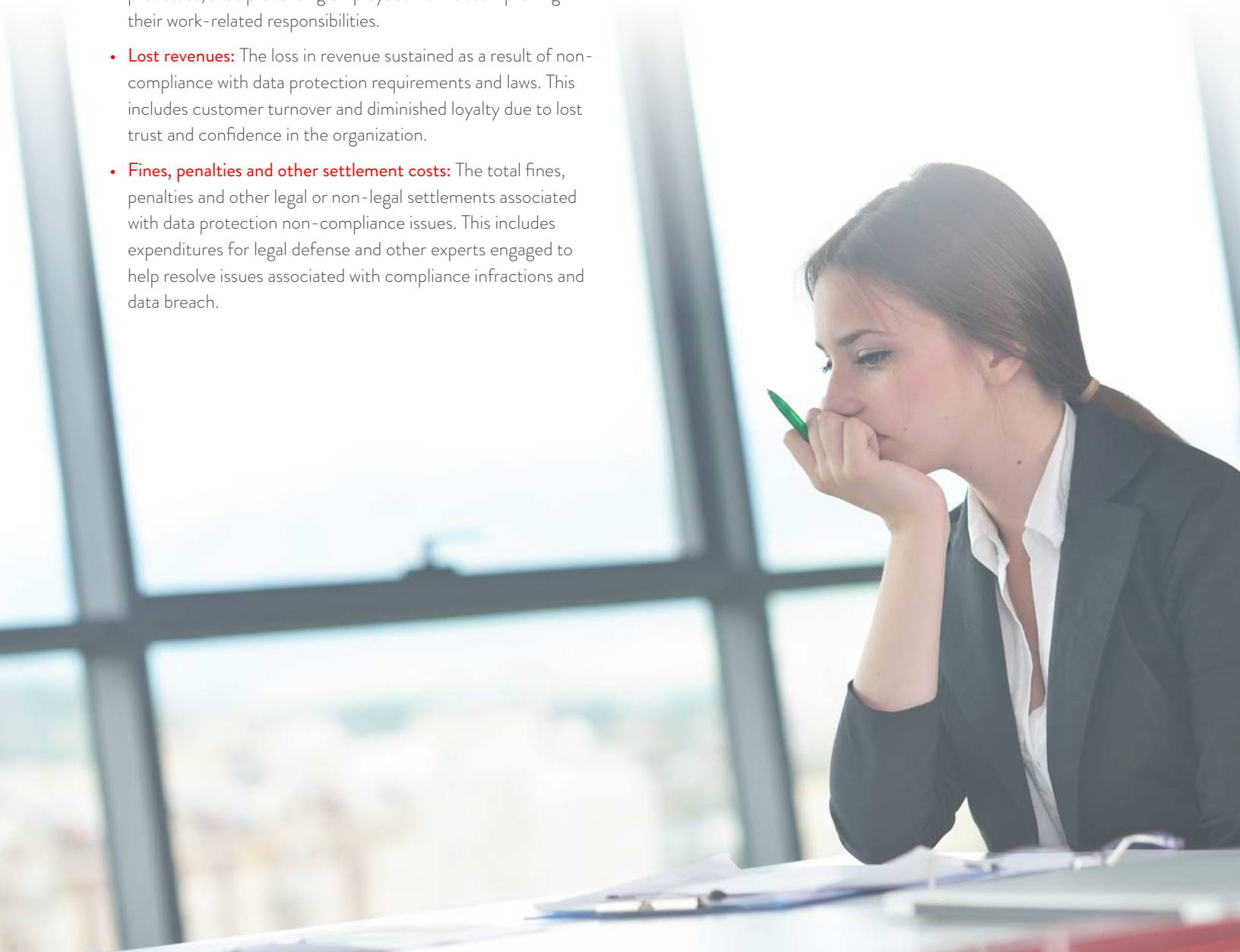
- Data compliance policies: Activities associated with the creation and dissemination of policies that pertain to the protection of confidential or sensitive information such as customer data, employee records, financial information, intellectual properties and others.
- Communications: Activities and associated costs that enable a company to train or create awareness of the organization's policies and related procedures for protecting sensitive or confidential information. This activity includes all downstream communications to employees, temporary employees, contractors and business partners. It also includes the required notifications about policy changes and data breach incidents.
- Program management: Activities and associated costs that relate to the coordination and governance of all program activities within the enterprise, including direct and indirect costs relating to privacy and IT compliance.
- Data security: All activities and technologies used by the organization to protect information assets. Activities include professional security staffing, implementation of control systems, backup and disaster recovery operations and others.
- Compliance monitoring: All activities deployed by the organization to assess or appraise compliance with external, internal and contractual obligations. It includes costs associated with internal audits, third-party audits, verification programs, professional audit staffing, audit technologies and others.
- Enforcement: Activities that relate to the detection of non-compliance, including incident response. It also includes redress activities such as hotlines, remedial training of employees who violate compliance requirements and voluntary self-reporting to regulators.

In addition to the above internal activities, most companies incur tangible costs and opportunity losses as a result of non-compliance with data protection requirements and laws. An example of a non-compliance event includes end-user violations of company policies such as the misuse of Internet applications or use of insecure devices in the workplace. Other examples include contractual violations with vendors or business partners, organizational changes imposed by regulators, data loss incidents, theft of intellectual properties and many others. Our total compliance cost framework includes the four broadly defined consequences of non-compliance as follows:

- Business disruption: The total economic loss that results from non-compliance events or incidents such as the cancellation of contracts, business process changes imposed by regulators, shutdowns of business operations, and others.
- Productivity loss: The lost time and related expenses associated with the downtime of systems and other critical processes, thus preventing employees from accomplishing their work-related responsibilities.
- Lost revenues: The loss in revenue sustained as a result of non-compliance with data protection requirements and laws. This includes customer turnover and diminished loyalty due to lost trust and confidence in the organization.
- Fines, penalties and other settlement costs: The total fines, penalties and other legal or non-legal settlements associated with data protection non-compliance issues. This includes expenditures for legal defense and other experts engaged to help resolve issues associated with compliance infractions and data breach.

We used an activity-based costing framework, which consists of six discernible cost center activities termed "compliance costs" and four discernible cost consequences termed "non-compliance costs." As shown, the six compliance costs are policy, communications, program management, data security, compliance monitoring and enforcement.

Each one of these activities generates direct, indirect and opportunity costs. The consequences for failing to comply with data compliance requirements include business disruption, productivity losses, revenue losses and fines, penalties and other cash outlays. Both sets of costs comprise the total cost of compliance, which is compiled for each benchmarked organization.



APPENDIX

BENCHMARK METHODS

To obtain information about each organization's total compliance cost, the researchers utilized an activity-based costing method and a proprietary diagnostic interviewing technique. Following are the approximate titles of 160 functional leaders in benchmarked organizations participating in our study:

- Chief information officer
- Chief information security officer
- Chief compliance officer
- Chief financial officer
- Chief privacy officer
- Internal audit director
- IT compliance leader
- IT operations leader
- Human resource leader
- Data center management

The benchmark instrument contains descriptive cost for each one of the six cost activity centers. Within each activity center, the survey requires respondents to estimate the cost range to signify direct cost, indirect cost and opportunity cost, defined as follows:

- **Direct cost:** the direct expense outlay to accomplish a given activity.
- **Indirect cost:** the amount of time, effort and other organizational resources spent, but not as a direct cash outlay.
- **Opportunity cost:** the cost resulting from lost business opportunities as a result of compliance infractions that diminish the organization's reputation and goodwill.

Our research methods captured information about all costs grouped into six core compliance activities:

- Policy development and upstream communication
- Training, awareness and downstream communication
- Data protection program activities
- Data security practices and controls
- Compliance monitoring and auditing
- Enforcement

Our benchmark instrument was designed to collect descriptive information from individuals who are responsible for data protection efforts within their organizations. The research design relies upon a shadow-costing method used in applied economic research. This method does not require subjects to provide actual accounting results, but instead relies on broad estimates based on the experience of individuals within participating organizations. Hence, we extrapolated the costs incurred by each organization either directly or indirectly to achieve compliance with a plethora of data protection requirements. Our methods also permitted us to collect information about the economic consequences of non-compliance as defined in the above.

The benchmark framework presents the two separate cost streams used to measure the total cost of data compliance for each participating organization. These two cost streams pertain to cost center activities and after-the-fact consequences experienced by organizations during or after a non-compliance event. Our benchmark instrument also contained questions designed to elicit the actual experiences and consequences of each incident. This cost study is unique in addressing the core systems and business activities that drive a range of expenditures associated with a company's efforts to comply with known requirements.

Within each category, cost estimation is a two-stage process. First, the survey requires individuals to provide direct cost estimates for each cost category by checking a range variable. A range variable is used rather than a point estimate to preserve confidentiality (in order to ensure a higher response rate). Second, the survey requires participants to provide a second estimate for both indirect cost and opportunity cost, separately. These estimates are calculated based on the relative magnitude of these costs in comparison to a direct cost within a given category. Finally, we conduct a follow-up interview to validate the reasonableness of cost estimates provided by respondents (and to resolve potential discrepancies).

The size and scope of survey items is limited to known cost categories that cut across different industry sectors. In our experience, a survey focusing on process yields a higher response rate and better quality of results. We also use a paper instrument, rather than an electronic survey, to provide greater assurances of confidentiality.

To maintain complete confidentiality, the survey instrument does not capture company-specific information of any kind. Research materials do not contain tracking codes or other methods that could link responses to participating companies.

To keep the benchmark instrument to a manageable size, we carefully limited items to only those cost activities we consider crucial to the measurement of data compliance costs rather than all IT compliance costs. Based on discussions with learned experts, the final set of items focus on a finite set of direct or indirect cost activities. After collecting benchmark information, each instrument is examined carefully for consistency and completeness. In this study, two companies were rejected because of incomplete, inconsistent or blank responses.

The study was launched in April 2017 and fieldwork concluded in September 2017. The recruitment started with a personalized letter and a follow-up phone call to 209 organizations for possible participation in our study. While 71 organizations initially agreed to participate, 53 organizations permitted researchers to complete the benchmark analysis.

The time horizon used in the analysis of data compliance costs is a 12-month period. We collected information over approximately the same time frame; hence, this limits our ability to gauge seasonal variation on specific cost categories.

SOURCES

1. See: Cost of Compliance: Benchmark Study of Multinational Organizations (sponsored by Tripwire), Ponemon Institute January 2011.
2. The percentage net change calculation is defined as follows: (FY2017–FY2011) ÷ [(FY2017+FY2011)×½].)
3. Please note that all audits examined in this analysis were all internally conducted either by in-house or contract (outsourced) staff.
4. Ponemon Institute initially developed the Security Effectiveness Score in its 2005 Encryption Trends Study. The purpose of the SES is to define the security posture of responding organizations. The SES is derived from the rating of leading information security and data protection practices. This indexing method has been validated from more than 50 independent studies conducted since June 2005. The SES provides a range of +2 (most favorable) to -2 (least favorable). An index value above zero is net favorable.
5. Ponemon Institute's cost of data breach studies conducted over the past 12 years utilizes activity-based cost to define the total economic impact of data loss or theft that requires notification. See, for example, 2017 Cost of Data Breach, (sponsored by IBM) Ponemon Institute May 2017.

MAKE BUSINESS FLOW BRILLIANTLY

Globalscape, Inc. (NYSE MKT: GSB) is a pioneer in securing and automating the movement and integration of data seamlessly in, around and outside your business, between applications, people and places, in and out of the cloud. Whether you are a line-of-business stakeholder struggling to connect multiple cloud applications or an IT professional tasked with integrating partner data into homegrown or legacy systems, Globalscape provides cloud services that automate your work, secure your data and integrate your applications – while giving visibility to those who need it. Globalscape makes business flow brilliantly. For more information, visit **www.globalscape.com** or follow the blog and Twitter updates.

PONEMON INSTITUTE

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

To learn more about Globalscape and how its solutions can help organizations maintain compliance, please contact:

GlobalSCAPE, Inc. (GSB)
Corporate Headquarters
4500 Lockhill-Selma Rd, Suite 150
San Antonio, TX 78249, USA
Sales: 210-308-8267 / Toll Free: 800-290-5054
Technical Support: 210-366-3993
Web Support: www.globalscape.com/support

If you have questions or comments about this report, please contact us by letter, phone call or email:

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City, Michigan 49686 USA
1.800.887.3118
research@ponemon.org

GLOBALSCAPE

2017

COST OF CYBER CRIME STUDY

INSIGHTS ON THE SECURITY INVESTMENTS THAT MAKE A DIFFERENCE

Ponemon INSTITUTE

Independently conducted by Ponemon Institute LLC
and jointly developed by Accenture

EXECUTIVE SUMMARY

Average annualized cost of cybersecurity (USD)

$11.7M

Percentage increase in cost of cybersecurity in a year

22.7%

Average number of security breaches each year

130

Percentage increase in average annual number of security breaches

27.4%

PRIORITIZING BREAKTHROUGH INVESTMENTS

Over the last two years, the accelerating cost of cyber crime means that it is now 23 percent more than last year and is costing organizations, on average, US$11.7 million. Whether managing incidents themselves or spending to recover from the disruption to the business and customers, organizations are investing on an unprecedented scale—but current spending priorities show that much of this is misdirected toward security capabilities that fail to deliver the greatest efficiency and effectiveness.

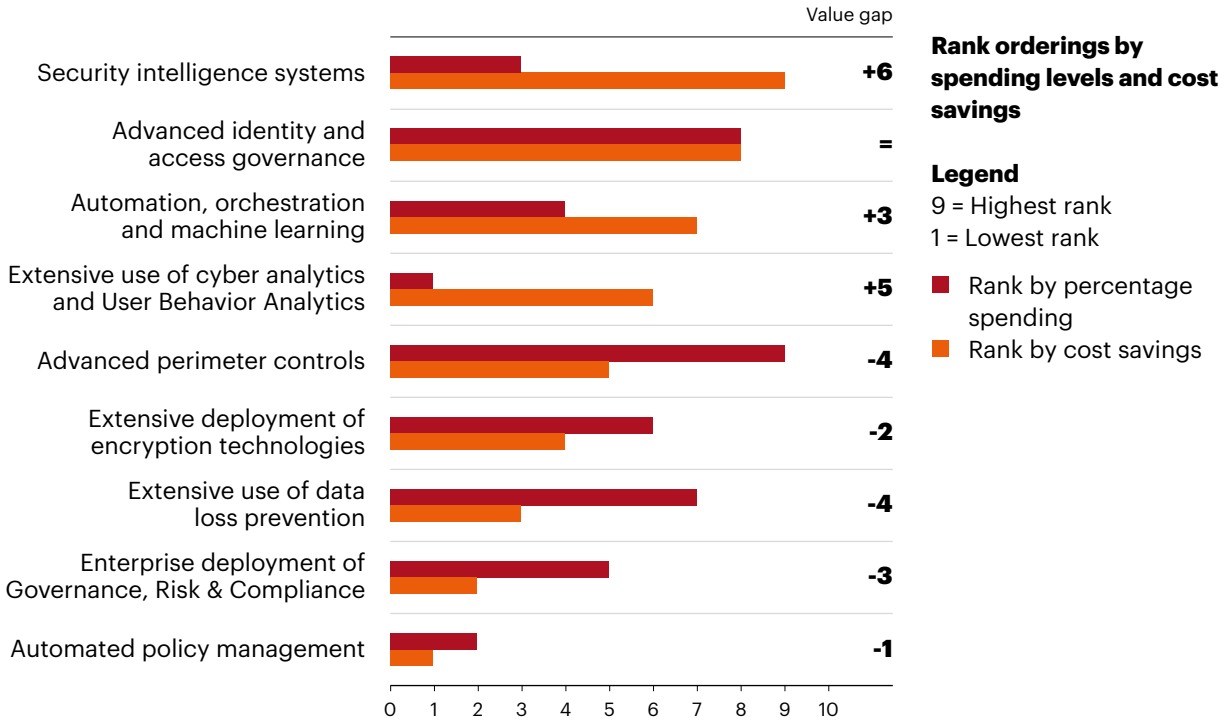
A better understanding of the cost of cyber crime could help executives bridge the gap between their own defenses and the escalating creativity—and numbers—of threat actors. Alongside the increased cost of cyber crime—which runs into an average of more than US$17 million for organizations in industries like Financial Services and Utilities and Energy—attackers are getting smarter. Criminals are evolving new business models, such as ransomware-as-a-service, which mean that attackers are finding it easier to scale cyber crime globally.

EXECUTIVE SUMMARY

With cyber attacks on the rise, successful breaches per company each year has risen more than 27 percent, from an average of 102 to 130. Ransomware attacks alone have doubled in frequency, from 13 percent to 27 percent, with incidents like WannaCry and Petya affecting thousands of targets and disrupting public services and large corporations across the world. One of the most significant data breaches in recent years has been the successful theft of 143 million customer records from Equifax—a consumer credit reporting agency—a cyber crime with devastating consequences due to the type of personally identifiable information stolen and knock-on effect on the credit markets. Information theft of this type remains the most expensive consequence of a cyber crime. Among the organizations we studied, information loss represents the largest cost component with a rise from 35 percent in 2015 to 43 percent in 2017. It is this threat landscape that demands organizations re-examine their investment priorities to keep pace with these more sophisticated and highly motivated attacks.

To better understand the effectiveness of investment decisions, we analyzed nine security technologies across two dimensions: the percentage spending level between them and their value in terms of cost-savings to the business. The findings illustrate that many organizations may be spending too much on the wrong technologies. Five of the nine security technologies had a negative value gap where the percentage spending level is higher than the relative value to the business. Of the remaining four technologies, three had a significant positive value gap and one was in balance. So, while maintaining the status quo on advanced identity and access governance, the opportunity exists to evaluate potential over-spend in areas which have a negative value gap and rebalance these funds by investing in the breakthrough innovations which deliver positive value.

THE POSITIVE OR NEGATIVE VALUE GAPS ASSOCIATED WITH SECURITY INVESTMENTS



Following on from the first *Cost of Cyber Crime*[1] report launched in the United States eight years ago, this study, undertaken by the Ponemon Institute and jointly developed by Accenture, evaluated the responses of 2,182 interviews from 254 companies in seven countries—Australia, France, Germany, Italy, Japan, United Kingdom and the United States. We aimed to quantify the economic impact of cyber attacks and observe cost trends over time to offer some practical guidance on how organizations can stay ahead of growing cyber threats.

1: The study examines the total costs organizations incur when responding to cyber crime incidents. These include the costs to detect, recover, investigate and manage the incident response. Also covered are the costs that result in after-the-fact activities and efforts to contain additional costs from business disruption and the loss of customers. These costs do not include the plethora of expenditures and investments made to sustain an organization's security posture or compliance with standards, policies and regulations.

EXECUTIVE SUMMARY

HIGHLIGHTS FROM THE FINDINGS INCLUDE:

Organizations need to better balance investments in security technologies.

Security intelligence systems (67 percent) and advanced identity and access governance (63 percent) are the top two most widely deployed enabling security technologies across the enterprise. They also deliver the highest positive value gap with organizational cost savings of US$2.8 million and US$2.4 million respectively. As the threat landscape constantly evolves, these investments should be monitored closely so that spend is at an appropriate level and maintains effective outcomes. Aside from systems and governance, other investments show a lack of balance. Of the nine security technologies evaluated, the highest percentage spend was on advanced perimeter controls. Yet, the cost savings associated with technologies in this area were only fifth in the overall ranking with a negative value gap of minus 4. Clearly, an opportunity exists here to assess spending levels and potentially reallocate investments to higher-value security technologies.

Compliance technology is important but don't bet the business on it.

Spending on governance, risk and compliance (GRC) technologies is not a fast-track to increased security. Enterprise-wide deployment of GRC technology and automated policy management showed the lowest effectiveness in reducing cyber crime costs (9 percent and 7 percent respectively) out of nine enabling security technologies. So, while compliance technology is important, organizations must spend to a level that is appropriate to achieve the required

capability and effectiveness, enabling them to free up funds for breakthrough innovations.

Organizations need to grasp the innovation opportunity.

Innovations are generating the highest returns on investment, yet investment in them is low. For example, two enabling security technology areas identified as "Extensive use of cyber analytics and User Behavior Analytics (UBA)" and "Automation, orchestration and machine learning" were the lowest ranked technologies for enterprise-wide deployment (32 percent and 28 percent respectively) and yet they provide the third and fourth highest cost savings for security technologies. By balancing investments from less rewarding technologies into these breakthrough innovation areas, organizations could improve the effectiveness of their security programs.

RECOMMENDATIONS

$2.8M cost savings from security intelligence systems and most positive value gap

The foundation of a strong and effective security program is to identify and "harden" the higher-value assets. These are the "crown jewels" of a business—the assets most critical to operations, subject to the most stringent regulatory penalties, and the source of important trade secrets and market differentiation. Hardening these assets makes it as difficult and costly as possible for adversaries to achieve their goals, and limits the damage they can cause if they do obtain access.

EXECUTIVE SUMMARY

By taking the following three steps, organizations can further improve the effectiveness of their cybersecurity efforts to fend off and reduce the impact of cyber crime:

1 > Build cyber-security on a strong foundation

Invest in the "brilliant basics" such as security intelligence and advanced access management and yet recognize the need to innovate to stay ahead of the hackers.

2 > Undertake extreme pressure testing

Organizations should not rely on compliance alone to enhance their security profile but undertake extreme pressure testing to identify vulnerabilities more rigorously than even the most highly motivated attacker.

3 > Invest in breakthrough innovation

Balance spend on new technologies, specifically analytics and artificial intelligence, to enhance program effectiveness and scale value.

Organizations need to recognize that spending alone does not always equate to value. Beyond prevention and remediation, if security fails, companies face unexpected costs from not being able to run their businesses efficiently to compete in the digital economy. Knowing which assets must be protected, and what the consequences will be for the business if protection fails, requires an intelligent security strategy that builds resilience from the inside out and an industry-specific strategy that protects the entire value chain. As this research shows, making wise security investments can help to make a difference.

$2.4 million average cost of malware attack spend and the top cost to companies

50 days average time to resolve a malicious insiders attack

23 days average time to resolve a ransomware attack

KEY FINDINGS

The average total cost by country, organizational size and industry

The financial consequence of a cyber attack is worsening. **P12**

The cost of cyber crime varies by organizational size. **P17**

Financial services has the highest cost of cyber crime. **P20**

The cost of cyber crime by type of attack

Certain attacks are more costly based on organizational size. **P21**

Ransomware attacks have doubled. **P23**

Country costs vary considerably by the type of cyber attack. **P24**

Costs vary significantly among countries. **P25**

The cost of cyber crime is also influenced by the frequency of attacks. **P26**

Malware and Web-based attacks are the two most costly attack types. **P27**

Malicious code attacks are taking longer to resolve and, as a result, are more costly. **P28**

Analysis of the costs to resolve the consequences of the cyber attack

Information theft remains the most expensive consequence of a cyber crime. **P29**

Companies spend the most on detection and recovery. **P30**

How companies allocate resources and achieve cost savings

Budget allocations are slowly shifting from the network to application and data layers. **P32**

Security intelligence systems have the biggest return on investment. **P35**

Maturity and effectiveness of an organization's security posture

Program maturity is weighted toward the middle stages. **P37**

Findings reveal a non-linear relationship between total cost of cyber crime and maturity stage of the cybersecurity program. **P38**

Two countries have a negative security effectiveness score. **P39**

The findings reveal a high SES decreases the total cost of cyber crime. **P40**

More investment is needed in breakthrough technologies. **P41**

The cost of cyber crime varies by country, organizational size, industry, type of cyber attack and maturity and effectiveness of an organization's security posture. In addition to presenting the range of costs according to these variables, we also analyzed the average expenditures and allocation of resources to resolve the cyber attack. Topics covered in this report include:

- Average total cost by country, organizational size and industry
- The cost of cyber crime by type of cyber attack
- Analysis of the costs to resolve the consequences of the cyber attack
- How companies allocate resources and achieve cost savings
- Maturity and effectiveness of an organization's security posture

KEY FINDINGS

The average total cost by country, organizational size and industry

KEY FINDING 1

The financial consequence of a cyber attack is worsening.

Figure 1 presents the global average cost of cyber crime over the last five years. After a steady increase for the first three years, the significant increase we uncovered last year has continued with an increase of 27.4 percent in the last year alone.

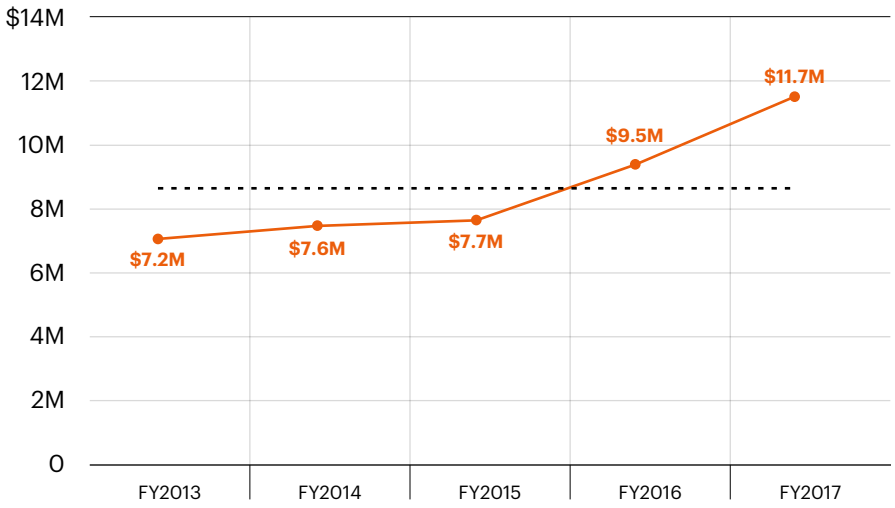


FIGURE 1
The global average cost of cyber crime over five years
US dollars

Legend
Consolidated view
n = 254 separate companies

Total average cost
Five-year average

Percentage change in average cost over five years is 62 percent

Figure 2 presents the estimated average cost of cyber crime for seven countries, involving 254 separate companies, for the past three years. Companies in the United States report the highest total average cost at US$21 million and Australia reports the lowest total average cost at US$5.41 million.

To determine the average cost of cyber crime, the 254 organizations in the study were asked to report what they spent to deal with cyber crimes experienced over four consecutive weeks. Once costs over the four-week period were compiled and validated, these figures were then grossed-up to determine the annualized cost.[2]

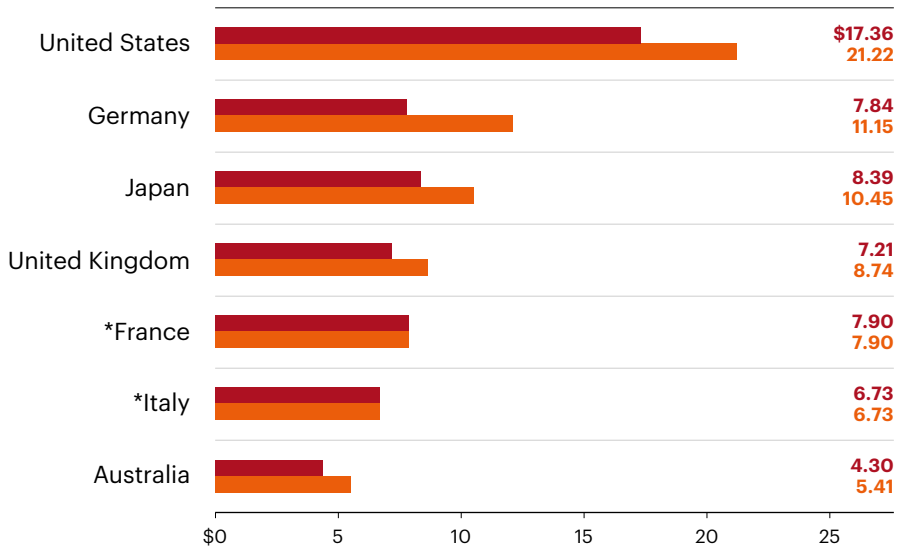


FIGURE 2
Total cost of cyber crime in seven countries
*Historical data does not exist for newly added country samples

Legend
US$ millions
n = 254

FY2016 (US$ millions)
FY 2017 (US$ millions)

2: Following is the gross-up statistic: Annualized revenue = [cost estimate]/[4/52 weeks].

KEY FINDINGS

Figure 3 summarizes the percentage increase in cyber crime costs between 2016 and 2017 as measured by the US dollar. As shown, Germany experienced the most significant increase in total cyber crime cost and the United Kingdom had the lowest change.

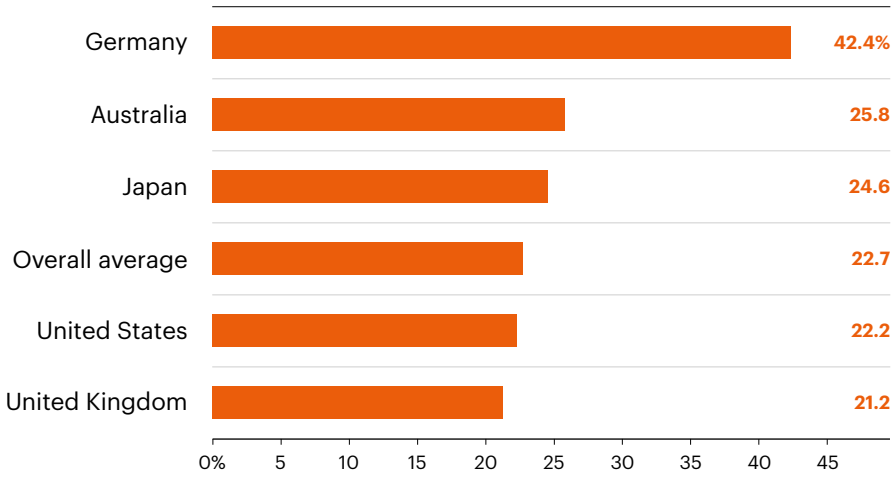


FIGURE 3
One-year percentage increase in cyber crime by country sample
Percentage increase could not be calculated for France and Italy as they were included for the first time in this report

Legend
Mean = 20.4%
n = 254 companies

Figure 4 reports the distribution of annualized total cost for 254 companies. As can be seen, 90 companies in our sample incurred total costs above the mean value of US$11.7 million, indicating a skewed distribution. The highest cost estimate of US$77.1 million was determined not to be an outlier based on additional analysis. A total of 163 organizations experienced an annualized total cost of cyber crime below the mean value.

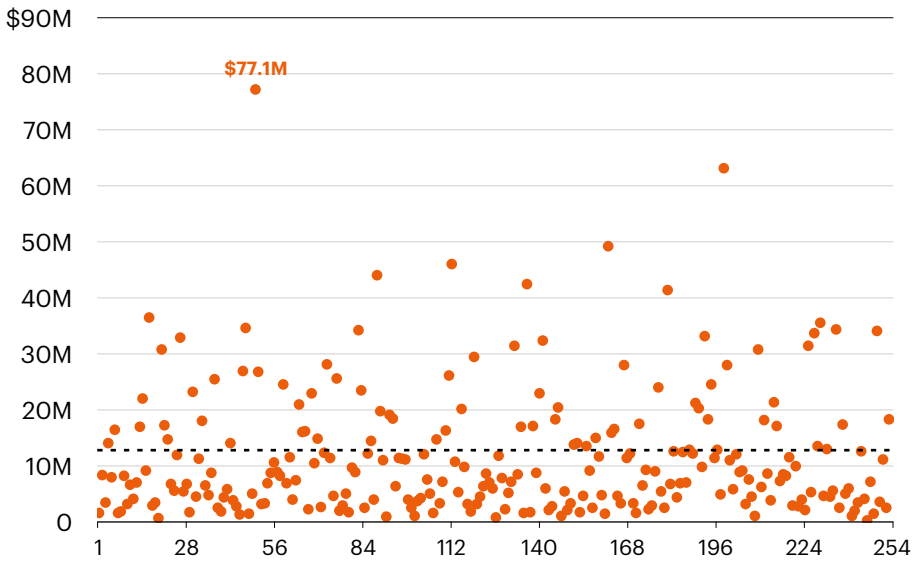


FIGURE 4
Scattergram of total cost of cyber crime for 254 participating companies
Cost expressed in US$

Legend
- 2017 Average total cost
- 2017 Annualized total cost

KEY FINDINGS

As part of our analysis we calculated a precision interval for the average cost of US$11.7 million. The purpose of this interval is to demonstrate that our cost estimates should be thought of as a range of possible outcomes, rather than a single point or number.

The range of possible cost estimates widens at increasingly higher levels of confidence, as shown in Figure 5. Specifically, at a 90 percent level of confidence we expect the range of cost to be between US$11 million to US$12.3 million.

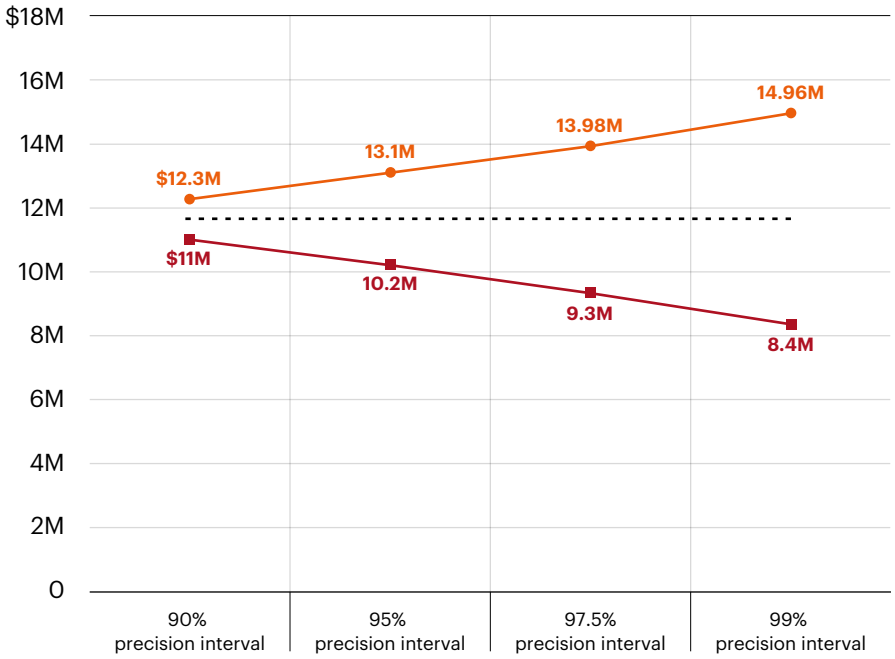


FIGURE 5
Precision interval for the mean value of annualized total cost
Cost expressed in US$

Legend
Minimum
Mean
Maximum

KEY FINDING 2

The cost of cyber crime varies by organizational size.

As shown in Figure 6, organizational size, as measured by the number of enterprise seats or nodes, is positively correlated to annualized cyber crime cost. This positive correlation is indicated by the upward sloping regression line. The number of seats ranges from a low of 1,050 to a high of 259,000.

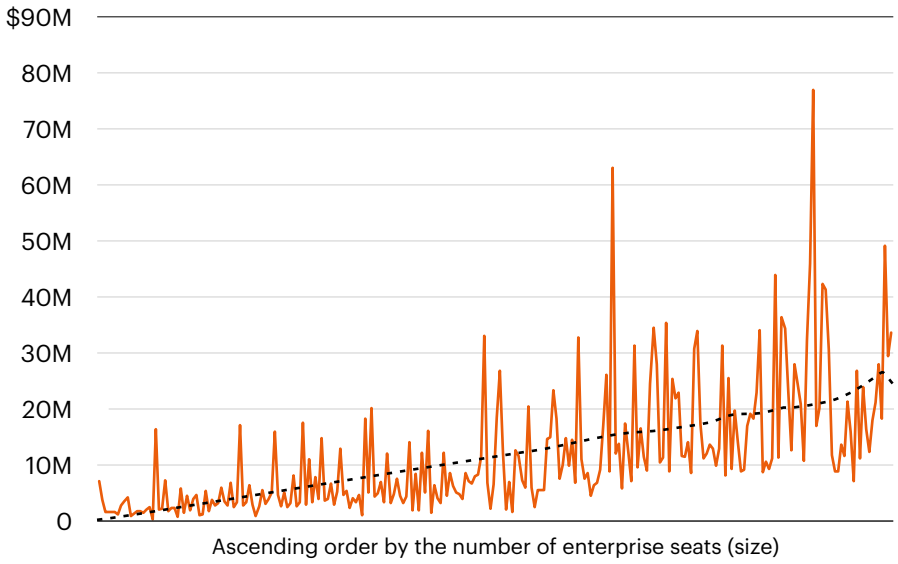


FIGURE 6
Annualized cost in ascending order by the number of enterprise seats
Cost expressed in US$

Legend
— 2017 Annualized total cost
--- Regression

KEY FINDINGS

Organizations are placed into one of four quartiles based on their total number of enterprise seats[3] (which we use as a size surrogate). We do this to create a more precise understanding of the relationship between organizational size and the cost of cyber crime. Table 1 shows the quartile average cost of cyber crime for three years. Approximately 64 companies are in each quartile.

TABLE 1
The quartile average cost of cyber crime over three years

TABLE 1 Quartile analysis	**FY 2017**	**FY 2016**	**FY 2015**	**FY 2014**	**FY 2013**
Cost expressed in US$	(n=254)	(n=237)	(n=252)	(n=257)	(n=234)
Quartile 1 (smallest)	$3,556,300	$3,477,633	$3,279,376	$2,967,723	$2,965,464
Quartile 2	$5,685,633	$5,567,110	$5,246,519	$5,107,532	$4,453,688
Quartile 3	$10,125,414	$9,854,250	$8,987,450	$8,321,024	$6,659,478
Quartile 4 (largest)	$16,852,250	$14,589,120	$13,372,861	$13,805,529	$14,707,980

3: Enterprise seats refer to the number of direct connections to the network and enterprise systems.

Table 2 reports the average cost per enterprise seat (also known as the per capita cost) compiled for four quartiles ranging from the smallest (Quartile 1) to the largest (Quartile 4). Consistent with prior years, the 2015 average per capita cost for organizations with the fewest seats is approximately four times higher than the average per capita cost for organizations with the most seats (US$1,726 versus US$436).

TABLE 2
The average cost per enterprise seat

TABLE 2 Quartile analysis	**2017 cost/seat**	**2016 cost/seat**	**2015 cost/seat**	**2014 cost/seat**	**2013 cost/seat**
Cost expressed in US$	(n=254)	(n=237)	(n=252)	(n=257)	(n=234)
Quartile 1 (smallest)	$1,726	$1,688	$1,555	$1,601	$1,388
Quartile 2	$975	$952	$878	$962	$710
Quartile 3	$655	$698	$709	$726	$532
Quartile 4 (largest)	$436	$401	$368	$437	$431

KEY FINDINGS

KEY FINDING 3

Financial services has the highest cost of cyber crime.

The average annualized cost of cyber crime varies by industry segment. In this year's study we compare cost averages for 15 different industry sectors. As shown in Figure 7, the cost of cyber crime for companies in financial services and utilities and energy have the highest annualized cost. In contrast, companies in life science, education and hospitality incurred a much lower cost on average.[4]

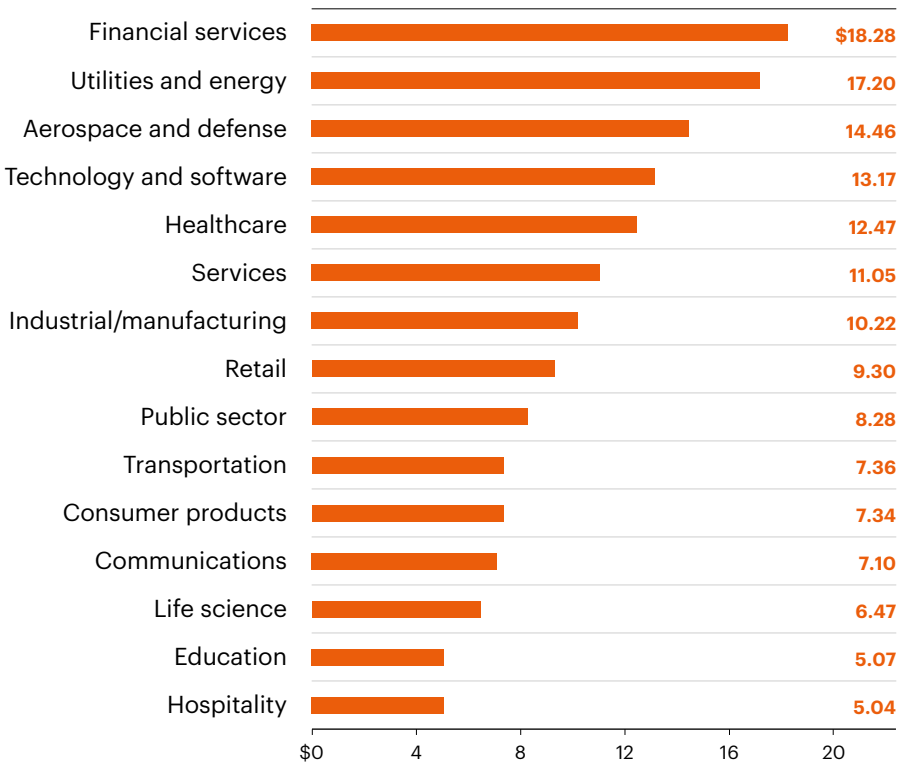


FIGURE 7
Average annualized cost by industry sector
US$ millions

Legend
Consolidated view
n = 254 companies

Total annualized cost ($1 million omitted)

4: This analysis is for illustration purposes only. The sample sizes in several sectors are too small to make definitive conclusions about industry differences.

The cost of cyber crime by type of attack

KEY FINDING 4

Certain attacks are more costly based on organizational size.

The study focuses on nine different attack vectors as the source of the cyber crime. In Figure 8, we compare smaller and larger-sized organizations based on the sample median of 8,560 seats.

Smaller organizations (below the median) experience a higher proportion of cyber crime costs relating to malware, Web-based attacks, phishing and social engineering attacks and stolen devices. In contrast, larger organizations (above the median) experience a higher proportion of costs relating to denial of services, malicious insiders and malicious code.

In the context of this research, malicious insiders include employees, temporary employees, contractors and, possibly other business partners. We also distinguish viruses from malware. Viruses reside on the endpoint and as yet have not infiltrated the network but malware has infiltrated the network. Malicious code attacks the application layer and includes SQL attack.

KEY FINDINGS

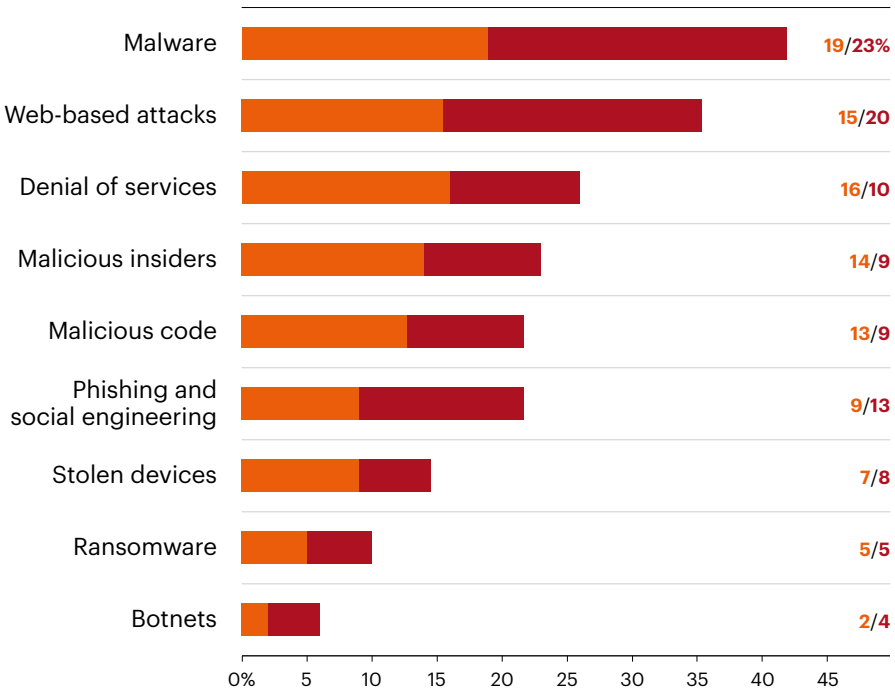


FIGURE 8
Organizational size affects the cost of nine attack types
Size measured according to the number of enterprise seats within the participating organizations

Legend
Consolidated view
n = 254 companies

- Above median number of enterprise seats
- Below median number of enterprise seats

This year, the benchmark sample of 254 organizations experienced a total of 635 discernible cyber attacks. Table 3 shows the number of successful attacks for the past six years, which has steadily increased.

TABLE 3
Frequency of discernible cyber attacks over six years

Year of study	Sample size	Total number of attacks	Successful attacks per company each week
FY 2017	254	635	2.5
FY 2016	237	465	2.0
FY 2015	252	477	1.9
FY 2014	257	429	1.7
FY 2013	234	343	1.4
FY 2012	199	262	1.3

KEY FINDING 5

Ransomware attacks have doubled.

Figure 9 summarizes in percentages the types of attack methods experienced by participating companies. As shown, ransomware attacks increased significantly from 13 percent to 27 percent since last year.

Virtually all organizations had attacks relating to viruses, worms and/or trojans and malware over the four-week benchmark period. Malware attacks and malicious code attacks are inextricably linked. We classified malware attacks that successfully infiltrated the organizations' networks or enterprise systems as a malicious code attack. Sixty-nine percent of companies experienced phishing and social engineering and 67 percent of companies had Web-based attacks. Malicious insiders increased from 35 percent in 2015 to 40 percent this year.

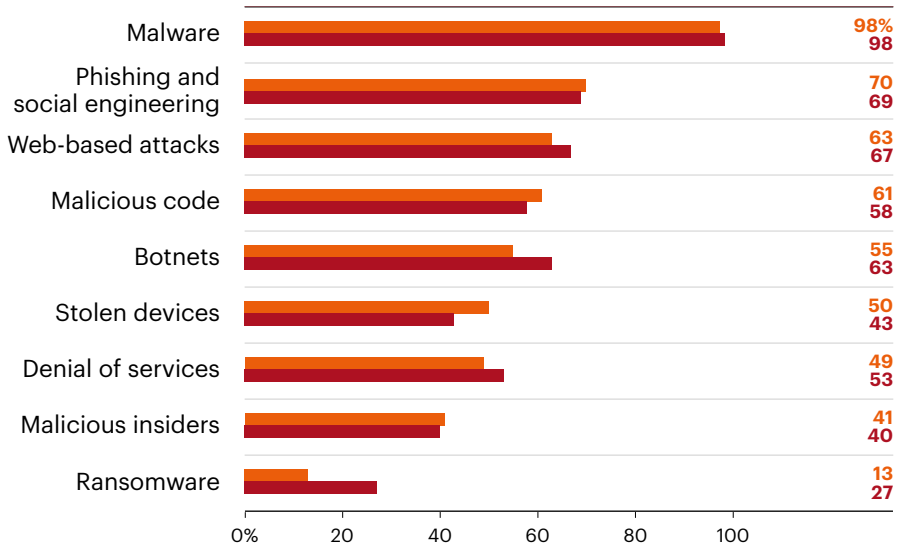


FIGURE 9
Types of cyber attacks experienced by companies

Legend
Consolidated view
n = 254 companies

FY 2016
FY 2017

KEY FINDINGS

KEY FINDING 6

Country costs vary considerably by the type of cyber attack.

Figure 10 compares benchmark results for seven countries, showing the percentage of annualized cost of cyber crime allocated to nine attack types compiled from all benchmarked organizations. Germany and Australia have the most costly malware attacks (both 23 percent), France has the most costly Web-based attacks (20 percent) and Germany and the United Kingdom have the most costly denial of service attacks (both 15 percent).

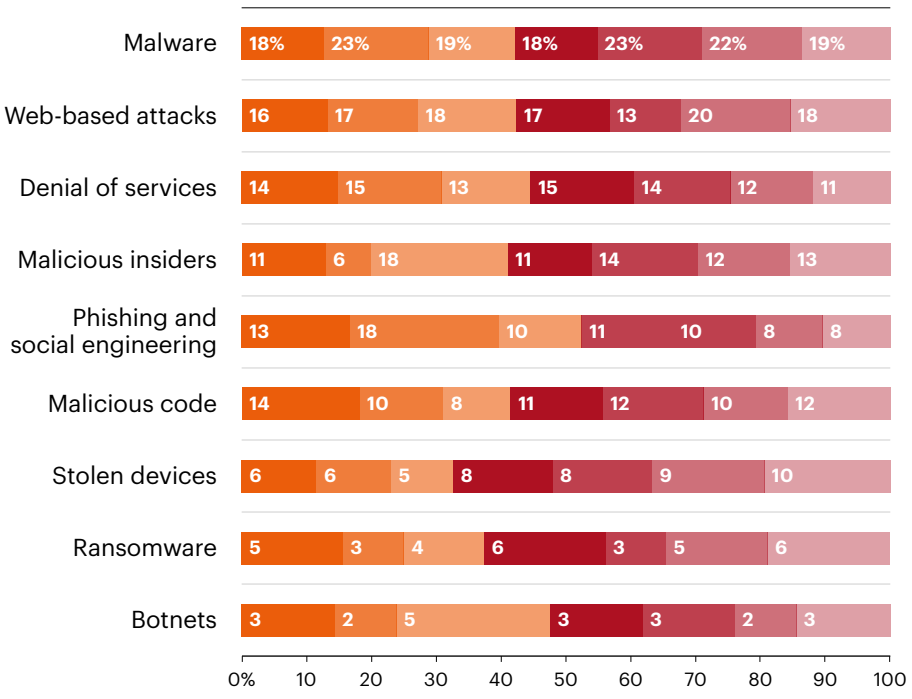


FIGURE 10
Percentage annualized cyber crime cost by attack type and country

Legend
Consolidated view
n = 254 companies

- United States
- Germany
- Japan
- United Kingdom
- Australia
- France
- Italy

KEY FINDING 7

Costs vary significantly among countries.

As shown in Figure 11, United States companies are paying more to resolve all types of cyber attack, especially for malware and Web-based attacks (US$3.82 million and US$3.40 million per attack, respectively). The least expensive attack type for all countries is a botnet.

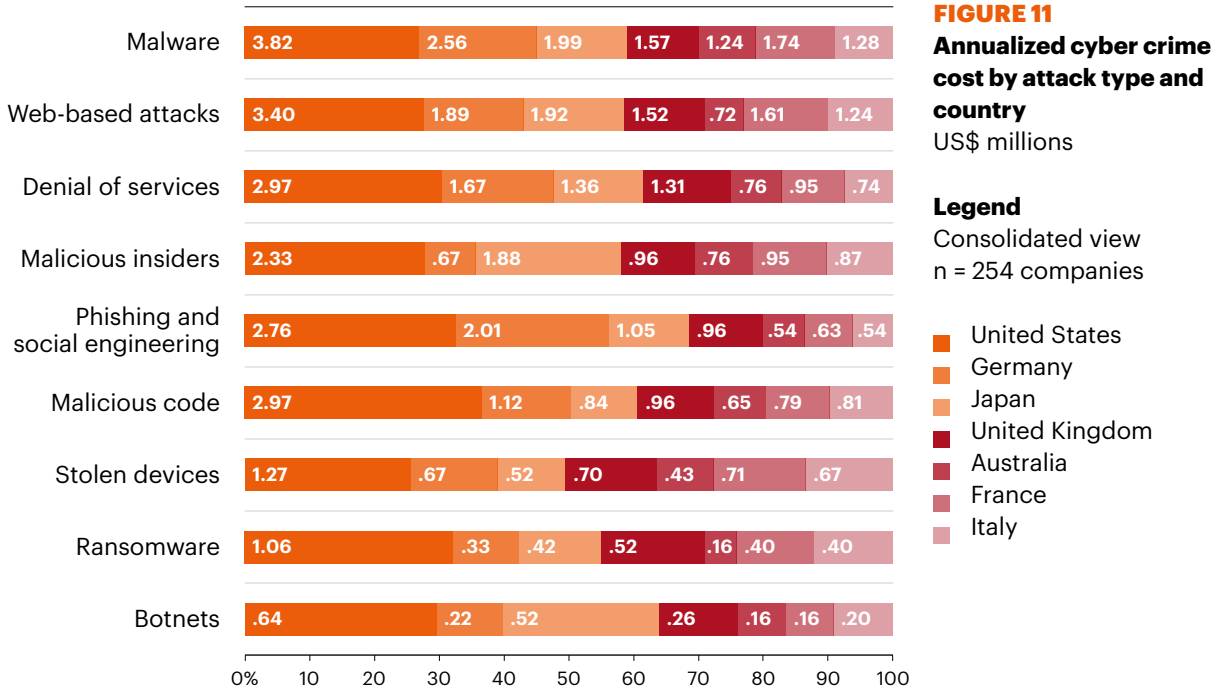


FIGURE 11
Annualized cyber crime cost by attack type and country
US$ millions

Legend
Consolidated view
n = 254 companies

KEY FINDINGS

KEY FINDING 8

The cost of cyber crime is also influenced by the frequency of attacks.

Figure 12 reveals the most to least expensive cyber attacks when analyzed by the frequency of incidents. The most expensive attacks are malicious insiders, denial of service and Web-based attacks.

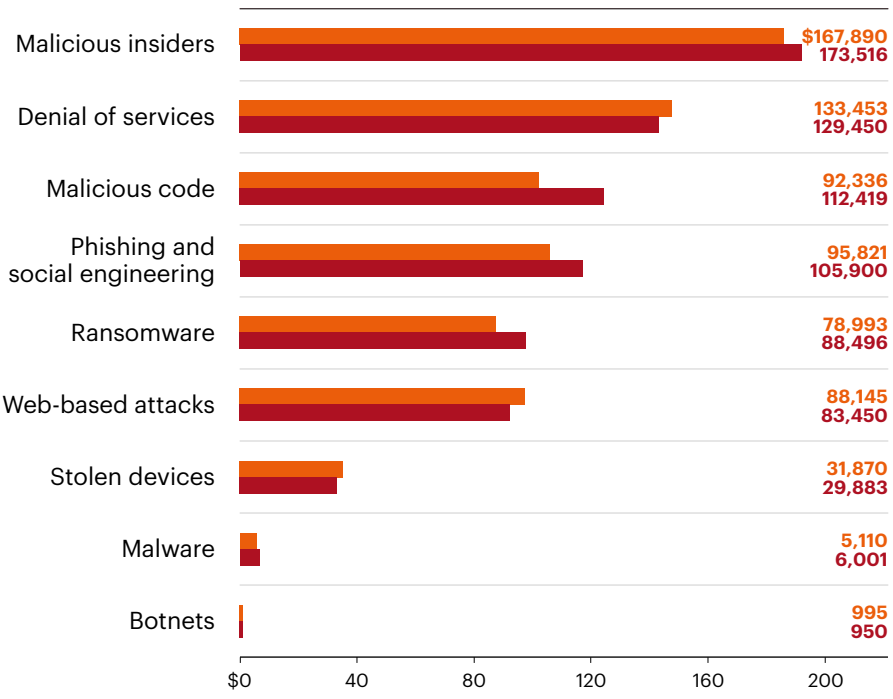


FIGURE 12
Average annualized cyber crime cost weighted by attack frequency

Legend
Consolidated view
n = 254 separate companies

FY 2016
FY 2017

KEY FINDING 9

Malware and Web-based attacks are the two most costly attack types.

As shown in Figure 13, companies spent an average of US$2.4 million and US$2 million on malware and Web-based attacks, respectively. Least costly are stolen devices, ransomware and botnets (US$865,985; US$532,914 and US$350,012, respectively).

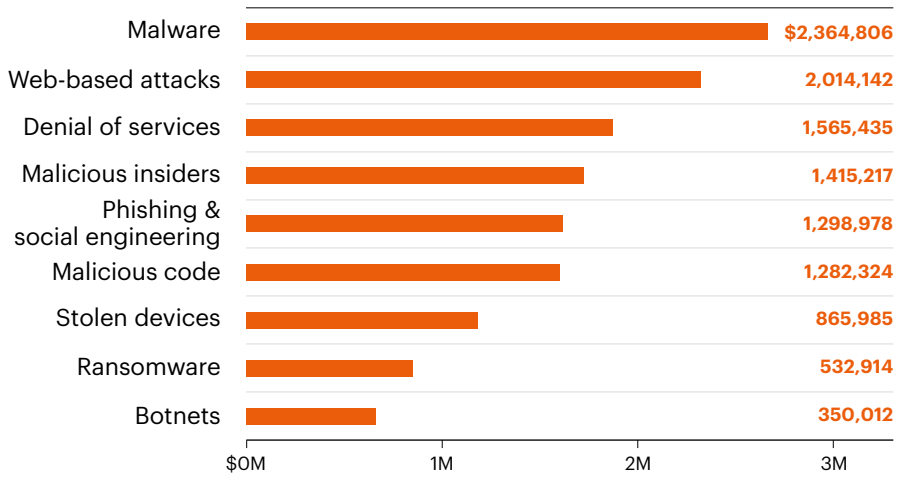


FIGURE 13
Total annualized cyber crime cost for attack types
US$ millions

Legend
Consolidated view
n = 254 separate companies

KEY FINDINGS

KEY FINDING 10

Malicious code attacks are taking longer to resolve and, as a result, are more costly.

As shown, the time it takes to resolve the consequences of the attack increases the cost of a cyber crime.

Figure 14 reports the average days to resolve cyber attacks for attack types studied in this report. It is clear from this chart that it takes the most amount of time, on average, to resolve attacks from malicious code, malicious insiders and ransomware (hackers). Malware, viruses and botnets on average are resolved relatively quickly (that is, in a few days). Since 2015, companies are spending more time to deal with malicious code (between 47.5 days and 55.2 days) and less time to deal with Web-based attacks (between 22.4 and 27.7 days).

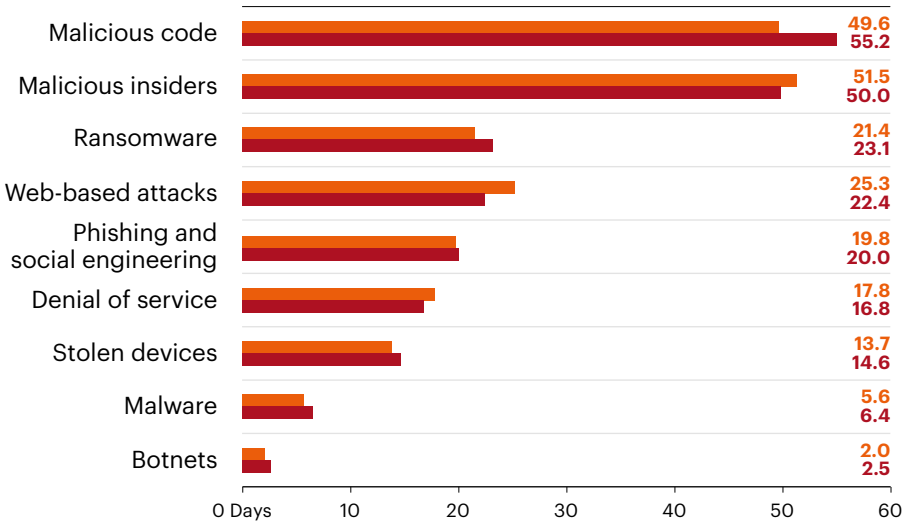


FIGURE 14
Length of time to resolve an attack in days
Estimated average time is measured for each attack type in days

Legend
Consolidated view
n = 254 separate companies

FY 2016
FY 2017

Analysis of the costs to resolve the consequences of the cyber attack

KEY FINDING 11

Information theft remains the most expensive consequence of a cyber crime.

In this research we look at four primary consequences of a cyber attack: business disruptions, the loss of information, loss of revenue and damage to equipment.

As shown in Figure 15, among the organizations represented in this study, information loss represents the largest cost component (43 percent). The cost of business disruption has decreased significantly from 39 percent in 2015 to 33 percent in this year's research. Business disruption costs include diminished employee productivity and business process failures that happen after a cyber attack. Revenue losses and equipment damages follow at 21 percent and 3 percent, respectively.

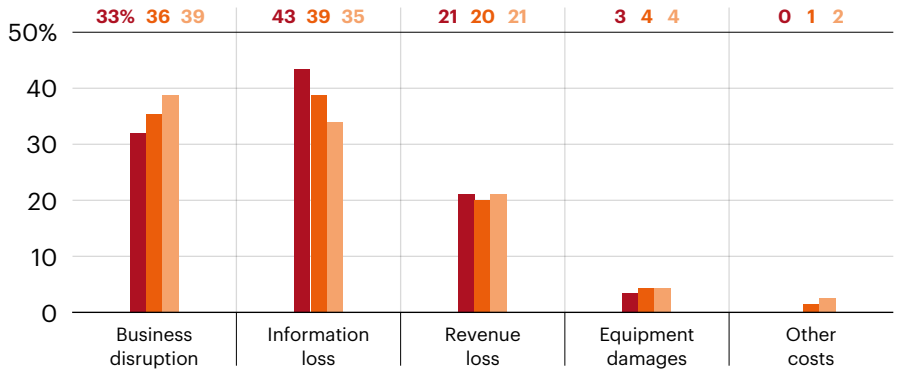


FIGURE 15
Percentage cost by consequence

Legend
Consolidated view
n = 254 separate companies

FY 2017
FY 2016
FY 2015

KEY FINDINGS

KEY FINDING 12

Companies spend the most on detection and recovery.

Cyber crime detection and recovery activities account for 55 percent of total internal activity cost (35 percent plus 20 percent), as shown in Figure 16. This is followed by containment and investigation cost (at 21 percent and 11 percent, respectively). While detection costs have increased since 2015, recovery costs have decreased. Detection and recovery cost elements highlight a significant cost-reduction opportunity for organizations that are able to systematically manage recovery and deploy enabling security technologies to help facilitate the detection process.

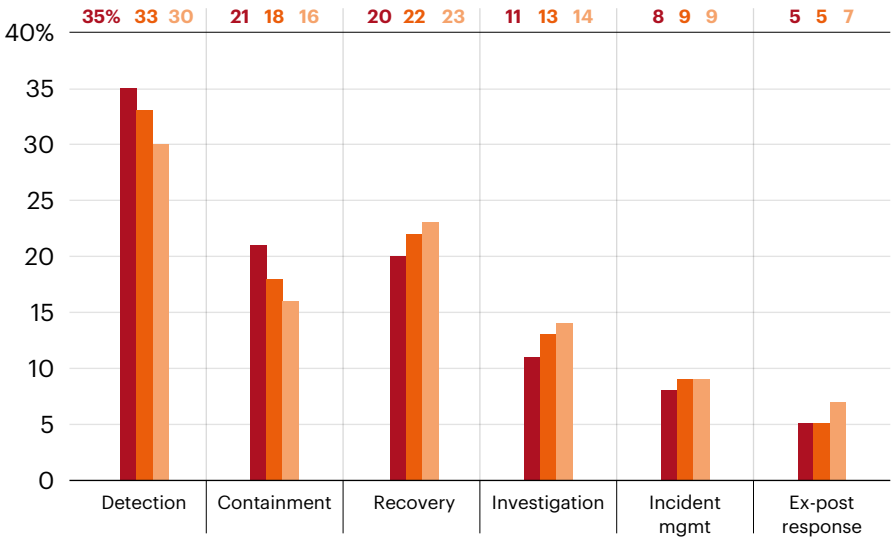


FIGURE 16
Percentage cost by internal activities

Legend
Consolidated view
n = 254 companies

FY 2017
FY 2016
FY 2015

The percentage of annualized costs can be further broken down into five specific expenditure components, which include: productivity loss (31 percent) direct labor (26 percent), cash outlays (20 percent), indirect labor (17 percent) and overhead (6 percent). Costs not included in these components are represented in the "other" category (Figure 17).

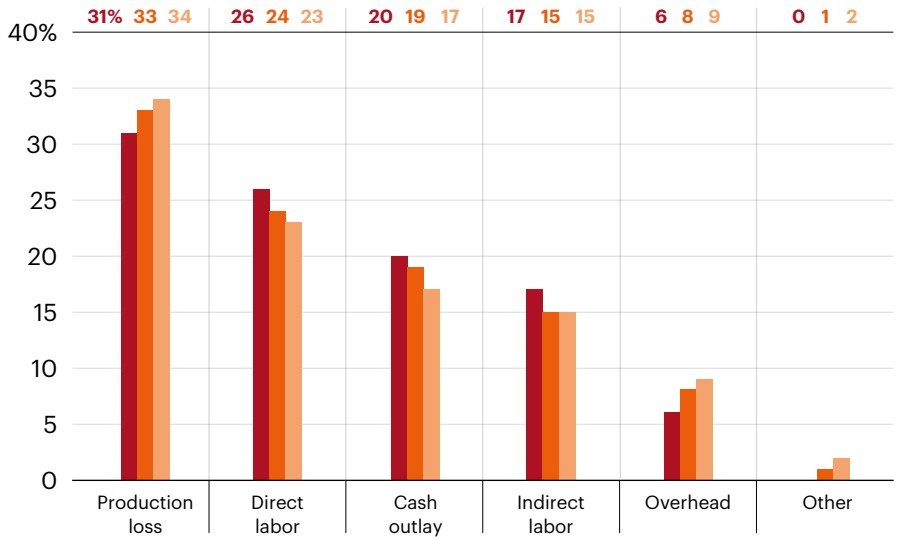


FIGURE 17
Percentage cost by specific components

Legend
Consolidated view
n = 254 companies

- FY 2017
- FY 2016
- FY 2015

How companies allocate resources and achieve cost savings

KEY FINDING 13

Budget allocations are slowly shifting from the network to application and data layers.

Figure 18 summarizes six layers in a typical multi-layered IT security infrastructure for all benchmarked companies. Each bar reflects the percentage dedicated spending according to the presented layer. The network layer receives the highest allocation at 27 percent of total dedicated IT security funding. At only six percent, the host layer receives the lowest funding level.

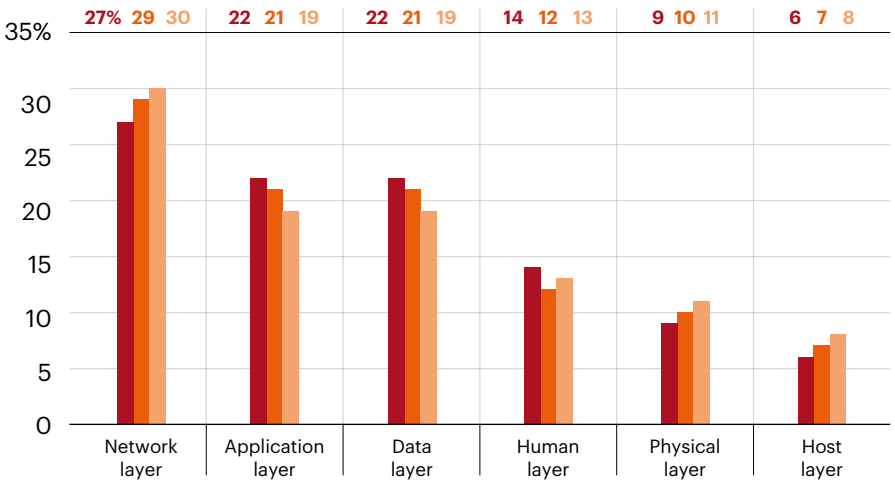


FIGURE 18
Percentage spending levels by six IT security layers

Legend
Consolidated view
n = 254 companies

- FY 2015
- FY 2016
- FY 2017

Figure 19 shows seven enabling security technology categories by a subset of benchmarked companies. Each bar represents the percentage of companies fully deploying each given security technology. The top three technology categories include: security intelligence systems (67 percent), access governance tools (63 percent), and advanced perimeter controls (58 percent). Cyber analytics and UBA and automation, orchestration and machine learning are not widely deployed (32 percent and 28 percent, respectively).

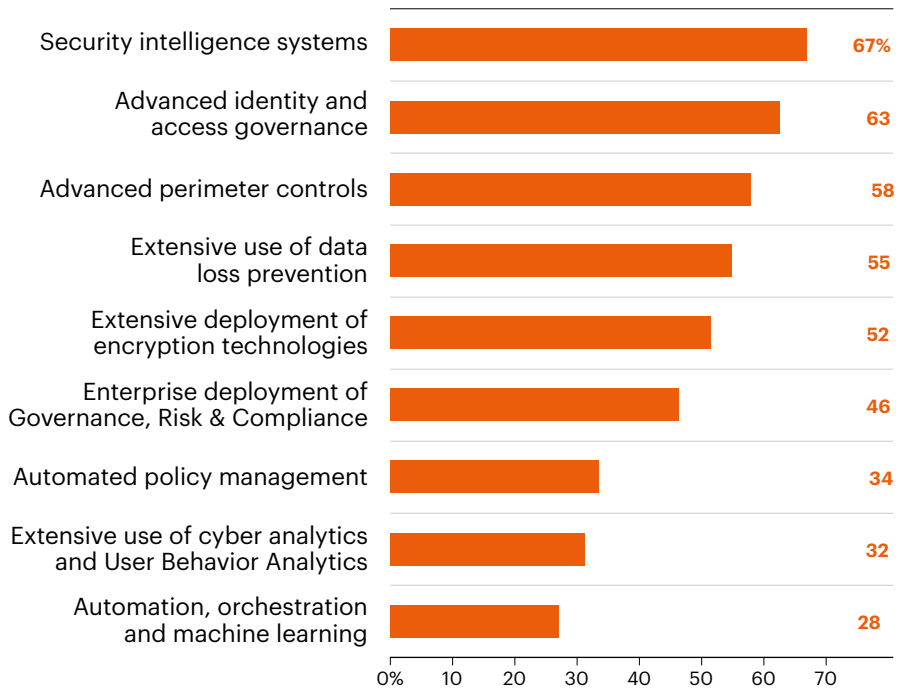


FIGURE 19
Seven enabling security technologies deployed

Legend
Consolidated view
n = 254 companies

Percentage deployment frequency

KEY FINDINGS

Figure 20 shows the money companies can save by deploying each one of seven enabling security technologies. For example, companies deploying security intelligence systems, on average, experience a substantial cost savings of US$2.8 million.

Similarly, companies deploying advanced identity and access governance tools experience cost savings of US$2.4 million on average. While not widely used, automation, organization and machine learning can provide significant cost savings (an average of US$2.4 million). Please note that these extrapolated cost savings are independent of each other and cannot be added together.

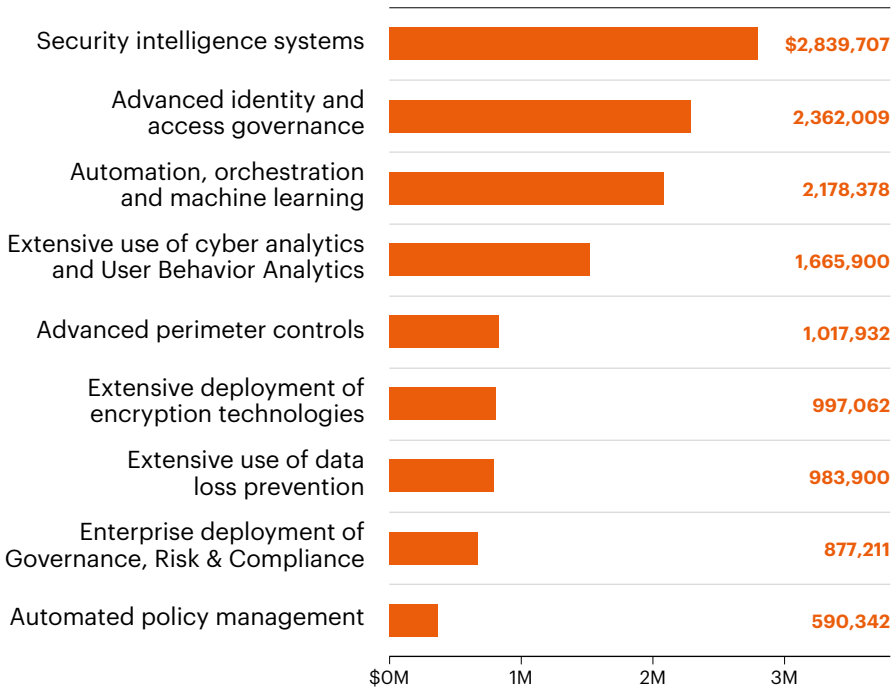


FIGURE 20
Cost savings when deploying enabling technologies

Legend
Consolidated view
n = 254 companies

Annual cost savings (US$)

KEY FINDING 14

Security intelligence systems have the biggest return on investment.

Figure 21 summarizes the estimated return on investment (ROI) realized by companies for each one of the nine categories of enabling security technologies.[5] At 21.5 percent, companies deploying security intelligence systems, on average, experience a substantially higher ROI than all other technology categories in this study.

Also significant are the estimated ROI results for companies that utilize advanced identity and access governance and automation, orchestration and machine learning technologies (19.7 percent and 17.1 percent, respectively). The estimated average ROI for all nine categories of enabling security technologies is 14.1 percent.

5: The return on investment calculated for each security technology category is defined as: (1) gains from the investment divided by (2) cost of investment (minus any residual value). We estimate a three-year life for all technology categories presented. Hence, investments are simply amortized over three years. The gains are the net present value of cost savings expected over the investment life. From this amount, we subtract conservative estimates for operations and maintenance cost each year. The net present value used the prime plus 2 percent discount rate per year. We also assume no (zero) residual value.

KEY FINDINGS

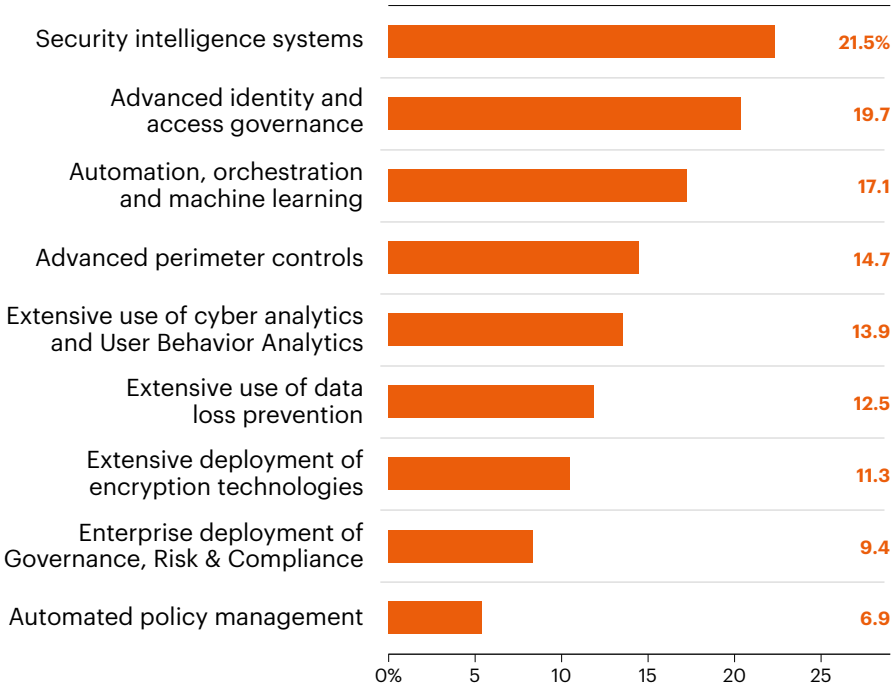


FIGURE 21
Estimated ROI for enabling security technologies

Legend
Consolidated view
n = 254 companies

- Estimated annual return on investment (ROI)

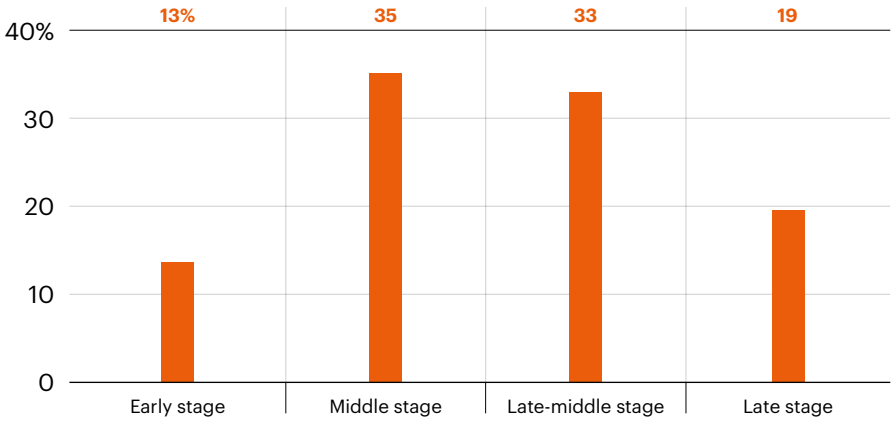


FIGURE 22
Distribution of the sample according to program maturity stage

Legend
n = 254 companies

- Stages of IT security program maturity

Maturity and effectiveness of an organization's security posture

KEY FINDING 15

Program maturity is weighted toward the middle stages.

Figure 22 reports the distribution of our global sample of 254 companies according one of four maturity stages of the cybersecurity program, defined as follows:

- Early stage—many cybersecurity program activities have not as yet been planned or deployed
- Middle stage—cybersecurity program activities are planned and defined but only partially deployed
- Late-middle stage—many cybersecurity program activities are deployed across the enterprise
- Mature stage—most cybersecurity program activities are deployed across the enterprise

As can be seen, 35 percent of the sample is located in the middle stage. Only 13 percent of the sample is located in the early stage. Another 19 percent is located in the late stage.

KEY FINDINGS

KEY FINDING 16

Findings reveal a non-linear relationship between total cost of cyber crime and maturity stage of the cybersecurity program.

As can be seen in Figure 23, organizations in the early stage experience the lowest total cost at US$8.32 million. Middle stage organizations experience the highest total cost at US$13.87 million.

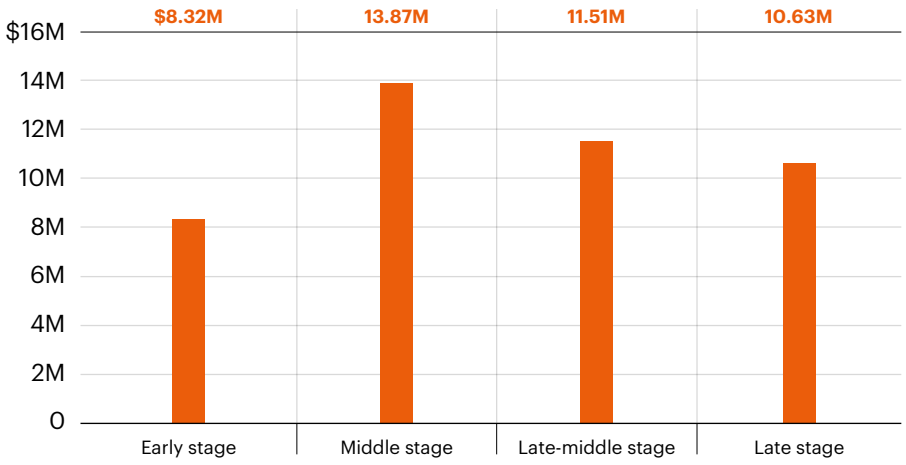


FIGURE 23
Total cost by program maturity stage

Legend
Mean = $11.7
n = 254 separate companies

Total cost (US$ millions)

KEY FINDING 17

Two countries have a negative security effectiveness score.

To better understand how security practises affect the total cost of cyber crime, we split the sample according to each company's security posture, which is measured by the Security Effectiveness Score (SES). Ponemon Institute developed this proprietary benchmarking methodology more than 10 years ago. The SES score is derived from rating numerous security practises, including the deployment of enabling security technologies.

This method has been validated from more than 50 independent studies conducted for more than a decade. The SES provides a range of +2 (most favorable) to -2 (least favorable) with a theoretical mean of zero. Hence, a score greater than zero is viewed as net favorable and a score less than zero is net unfavorable. A high favorable score (such as +1 or above) indicates that the organization's investment in people and technologies is both effective in achieving its security mission and is efficient in utilizing limited resources.

It is our belief that companies with a high SES are more cyber resilient and will have methods that will lessen the cost impact of cyber crimes. The mean SES for all 254 companies in our global sample is +.57. The highest SES was +1.76 and the lowest SES was -1.61. Figure 24 shows the mean SES by country sample. Germany achieved the highest overall SES at +1.03. In contrast, Italy had the lowest SES at -0.15. net favorable and a score less than zero is net unfavorable.

KEY FINDINGS

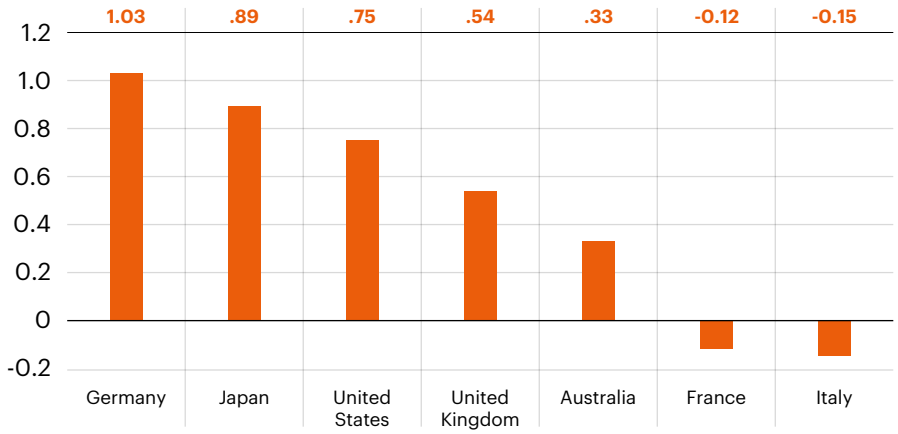


FIGURE 24
Average SES by country samples

Legend
Mean = +57
n = 254 separate companies

Security effectiveness score (SES)

KEY FINDING 18

The findings reveal a high SES decreases the total cost of cyber crime.

Organizations in the highest SES quartile experienced an average total cost of cyber crime at US$9.0 million. In contrast, organizations in the lowest SES quartile experienced an average total cost at US$15.3 million, as shown in Figure 25.

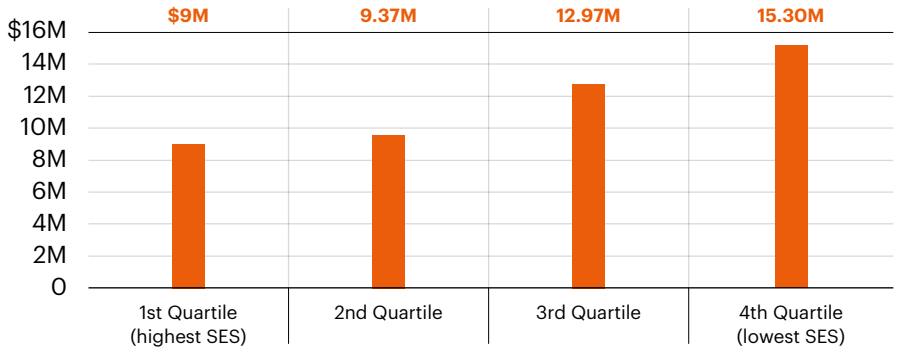


FIGURE 25
Total cost of cyber crime by SES quartile
US$ millions

Legend
Mean = $11.7
n = 254 separate companies

Total annualized cost ($US millions)

KEY FINDING 19

More investment is needed in breakthrough technologies.

Figure 26 presents the results of two independent rankings. The first ranking shows the order of nine (9) enabling security technologies as defined above. As shown, security intelligence systems provide the greatest cost savings, thus earning a rank equal to 9. In contrast, automated policy management provides the lowest savings, with a rank equal to 1.

The second ranking shows the order of enabling security technologies based on the percentage spending level during FY 2017. Here, security intelligence systems has a rank of 3 (third from the bottom). In terms of spending level, advanced perimeter controls has the highest rank of 9, but only a rank of 5 with respect to cost savings. Hence, differences or value gaps between these two rankings suggest possible inefficiencies in the allocation of resources on security solutions.

KEY FINDINGS

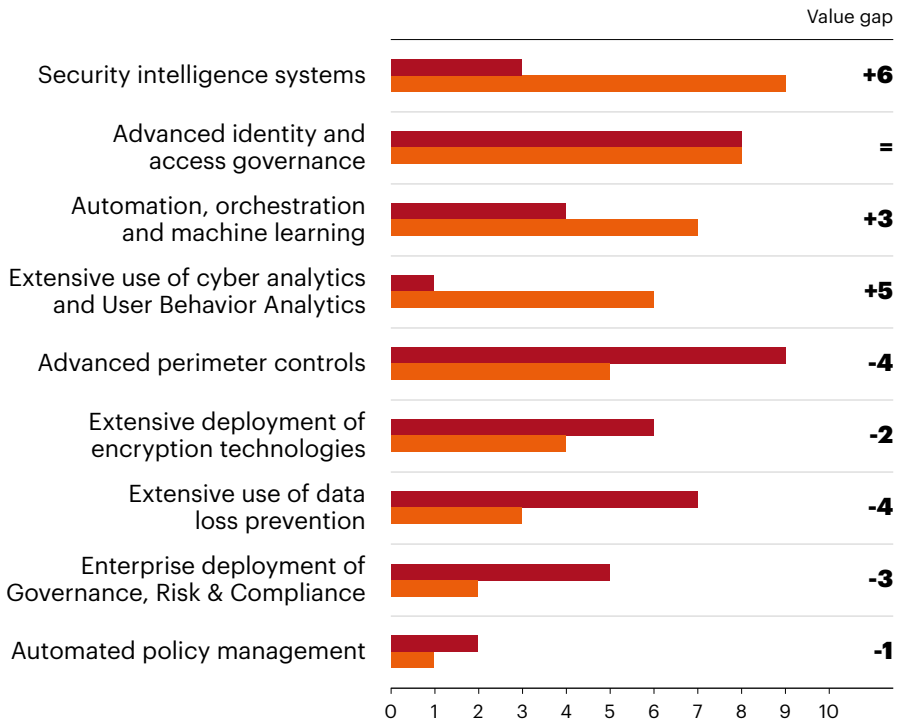


FIGURE 26
Rank orderings by spending levels and cost savings

Legend
9 = Highest rank
1 = Lowest rank

- Rank by percentage spending
- Rank by cost savings

ABOUT THE RESEARCH

COST OF CYBER CRIME
Frequently Asked Questions

What types of cyber attacks are included in this research?
For purposes of this study, we define cyber attacks as criminal activity conducted through the organization's IT infrastructure via the internal or external networks or the Internet. Cyber attacks also include attacks against industrial controls. A successful cyber attack is one that results in the infiltration of a company's core networks or enterprise systems. It does not include the plethora of attacks stopped by a company's firewall defenses.

How does benchmark research differ from survey research?
The unit of analysis in the *2017 Cost of Cyber Crime Study* is the organization. In survey research, the unit of analysis is the individual. In our experience, a traditional survey approach does not capture the necessary details required to extrapolate cyber crime costs. We conduct field-based research that involves interviewing senior-level personnel about their organizations' actual cyber crime incidents.

How do you collect the data?
In our 2017 study, our researchers collected in-depth qualitative data through 2,182 separate interviews conducted over a 10-month period in 254 companies in seven countries: the United States, the United Kingdom, Germany, France, Italy, Australia and Japan. In each of the 254 participating organizations, we spoke with IT, compliance and information security practitioners who are knowledgeable about the cyber attacks experienced by the company and the costs associated with resolving the cyber crime incidents. For privacy purposes we did not collect organization-specific information.

ABOUT THE RESEARCH

How do you calculate the cost?

To determine the average cost of cyber crime, organizations were asked to report what they spent to deal with cyber crimes over four consecutive weeks. Once the costs over the four-week period were compiled and validated, these figures were then grossed-up to determine the annualized cost. These are costs to detect, recover, investigate and manage the incident response. Also covered are the costs that result in after-the-fact activities and efforts to reduce business disruption and the loss of customers. These costs do not include expenditures and investments made to sustain an organization's security posture or compliance with standards, policies and regulations.

Are you tracking the same organizations each year?

For consistency purposes, our benchmark sample consists of only larger-sized organizations (that is, a minimum of approximately 1,000 enterprise seats).[6] Each annual study involves a different sample of companies. In short, we do not track the same sample of companies over time. To be consistent, we recruit and match companies with similar characteristics such as the company's industry, headcount, geographic footprint and size of data breach.

6: Enterprise seats refer to the number of direct connections to the network and enterprise systems.

Framework

The purpose of this research is to provide guidance on what a successful cyber attack can cost an organization. Our *2017 Cost of Cyber Crime Study* is unique in addressing the core systems and business process-related activities that drive a range of expenditures associated with a company's response to cyber crime. Cost figures have been converted into United States dollars for comparative purposes.[7]

In this study, we define a successful attack as one that results in the infiltration of a company's core networks or enterprise systems. It does not include the plethora of attacks stopped by a company's firewall defenses.

Figure 27 presents the activity-based costing framework used to calculate the average cost of cyber crime. Our benchmark methods attempt to elicit the actual experiences and consequences of cyber attacks. Based on interviews with a variety of senior-level individuals in each organization we classify the costs according to two different cost streams:

- The costs related to dealing with the cyber crime or what we refer to as the internal cost activity centers.
- The costs related to the consequences of the cyber attack or what we refer to as the external consequences of the cyber attack.

7: *The Wall Street Journal*'s August 16, 2017 currency conversion rates.

ABOUT THE RESEARCH

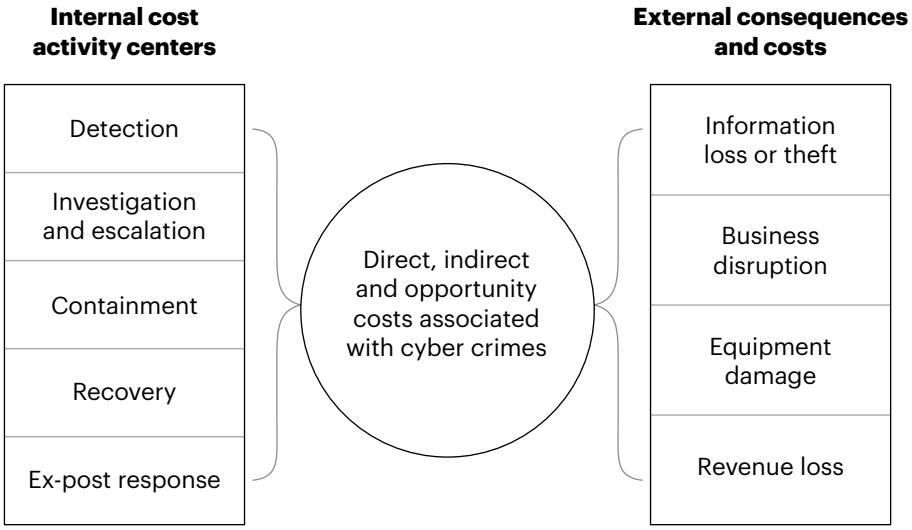


FIGURE 27
Cost framework for cyber crime

We analyzed the internal cost centers sequentially—starting with the detection of the incident and ending with the ex-post or final response to the incident, which involves dealing with lost business opportunities and business disruption. In each of the cost activity centers we asked respondents to estimate the direct costs, indirect costs and opportunity costs. These are defined as follows:

- Direct cost—the direct expense outlay to accomplish a given activity.
- Indirect cost—the amount of time, effort and other organizational resources spent, but not as a direct cash outlay.
- Opportunity cost—the cost resulting from lost business opportunities as a consequence of reputation diminishment after the incident.

External costs, including the loss of information assets, business disruption, equipment damage and revenue loss, were captured using shadow-costing methods. Total costs were allocated to nine discernible attack vectors: viruses, worms, trojans; malware; botnets;

Web-based attacks; phishing and social engineering; malicious insiders; stolen or damaged devices; malicious code (including SQL injection); and denial of services.[8]

This study addresses the core process-related activities that drive a range of expenditures associated with a company's cyber attack. The five internal cost activity centers in our framework include:[9]

Detection

Activities that enable an organization to reasonably detect and possibly deter cyber attacks or advanced threats. This includes allocated (overhead) costs of certain enabling technologies that enhance mitigation or early detection.

Investigation and escalation

Activities necessary to thoroughly uncover the source, scope, and magnitude of one or more incidents. The escalation activity also includes the steps taken to organize an initial management response.

Containment

Activities that focus on stopping or lessening the severity of cyber attacks or advanced threats. These include shutting down high-risk attack vectors such as insecure applications or endpoints.

8: We acknowledge that these nine attack categories are not mutually independent and they do not represent an exhaustive list. Classification of a given attack was made by the researcher and derived from the facts collected during the benchmarking process.
9: Internal costs are extrapolated using labor (time) as a surrogate for direct and indirect costs. This is also used to allocate an overhead component for fixed costs such as multi-year investments in technologies.

ABOUT THE RESEARCH

Recovery — Activities associated with repairing and remediating the organization's systems and core business processes. These include the restoration of damaged information assets and other IT (data center) assets.

Ex-post response — Activities to help the organization minimize potential future attacks. These include containing costs from business disruption and information loss as well as adding new enabling technologies and control systems.

In addition to the above process-related activities, organizations often experience external consequences or costs associated with the aftermath of successful attacks—which are defined as attacks that infiltrate the organization's network or enterprise systems. Accordingly, our research shows that four general cost activities associated with these external consequences are as follows:

Cost of information loss or theft — Loss or theft of sensitive and confidential information as a result of a cyber attack. Such information includes trade secrets, intellectual properties (including source code), customer information and employee records. This cost category also includes the cost of data breach notification in the event that personal information is wrongfully acquired.

Cost of business disruption

The economic impact of downtime or unplanned outages that prevent the organization from meeting its data processing requirements.

Cost of equipment damage

The cost to remediate equipment and other IT assets as a result of cyber attacks to information resources and critical infrastructure.

Lost revenue

The loss of customers (churn) and other stakeholders because of system delays or shutdowns as a result of a cyber attack. To extrapolate this cost, we use a shadow costing method that relies on the "lifetime value" of an average customer as defined for each participating organization.

Benchmarking

The cost of cyber crime benchmark instrument is designed to collect descriptive information from IT, information security and other key individuals about the actual costs incurred either directly or indirectly as a result of cyber attacks actually detected. Our cost method does not require subjects to provide actual accounting results, but instead relies on estimation and extrapolation from interview data over a four-week period.

ABOUT THE RESEARCH

Cost estimation is based on confidential diagnostic interviews with key respondents within each benchmarked organization. Table 4 reports the frequency of individuals by their approximate functional discipline that participated in this year's global study.

TABLE 4
Individuals participating in the 2017 global study by functional discipline

Functional areas of interview participants	FREQUENCY	PERCENTAGE (%)
IT security	385	18
IT operations	401	18
Compliance	198	9
Data center management	185	8
Accounting & finance	116	5
Network operations	118	5
Legal	99	5
IT risk management	110	5
Physical security/facilities mgmt	98	4
Human resources	95	4
Internal or IT audit	80	4
Application development	69	3
Enterprise risk management	70	3
Procurement/vendor management	59	3
Industrial control systems	56	3
Quality assurance	43	2
TOTAL	**2,182**	**100**
Interviews per company on average	8.59	

Data collection methods did not include actual accounting information, but instead relied upon numerical estimation based on the knowledge and experience of each participant. Within each category, cost estimation was a two-stage process. First, the benchmark instrument required individuals to rate direct cost estimates for each cost category by marking a range variable defined in the following number-line format.

The numerical value obtained from the number line, rather than a point estimate for each presented cost category, preserved confidentiality and ensured a higher response rate. The benchmark instrument also required practitioners to provide a second estimate for indirect and opportunity costs, separately.

Cost estimates were then compiled for each organization based on the relative magnitude of these costs in comparison to a direct cost within a given category. Finally, we administered general interview questions to obtain additional facts, including estimated revenue losses as a result of the cyber crime.

The size and scope of survey items was limited to known cost categories that cut across different industry sectors. In our experience, a survey focusing on process yields a higher response rate and better quality of results. We also used a paper instrument, rather than an electronic survey, to provide greater assurances of confidentiality.

To maintain complete confidentiality, the survey instrument did not capture company-specific information of any kind. Subject materials contained no tracking codes or other methods that could link responses to participating companies.

We carefully limited items to only those cost activities we considered crucial to the measurement of cyber crime cost to keep the benchmark

instrument to a manageable size. Based on discussions with learned experts, the final set of items focused on a finite set of direct or indirect cost activities. After collecting benchmark information, each instrument was examined carefully for consistency and completeness. In this study, a few companies were rejected because of incomplete, inconsistent or blank responses.

Field research was conducted over several months, concluding in August 2017. To maintain consistency for all benchmark companies, information was collected about the organizations' cyber crime experience was limited to four consecutive weeks. This time frame was not necessarily the same time period as other organizations in this study. The extrapolated direct, indirect and opportunity costs of cyber crime were annualized by dividing the total cost collected over four weeks (ratio = 4/52 weeks).

Sample

The recruitment of the annual study started with a personalized letter and a follow-up telephone call to 1,701 contacts for possible participation and 254 organizations permitted Ponemon Institute to perform the benchmark analysis.

Chart 1 summarizes the current (FY 2017) sample of participating companies based on 15 primary industry classifications. As can be seen, financial services (16 percent) represent the largest segment. This includes retail banking, insurance, brokerage and credit card companies. The second and third largest segments include industrial (12 percent) and services (11 percent).

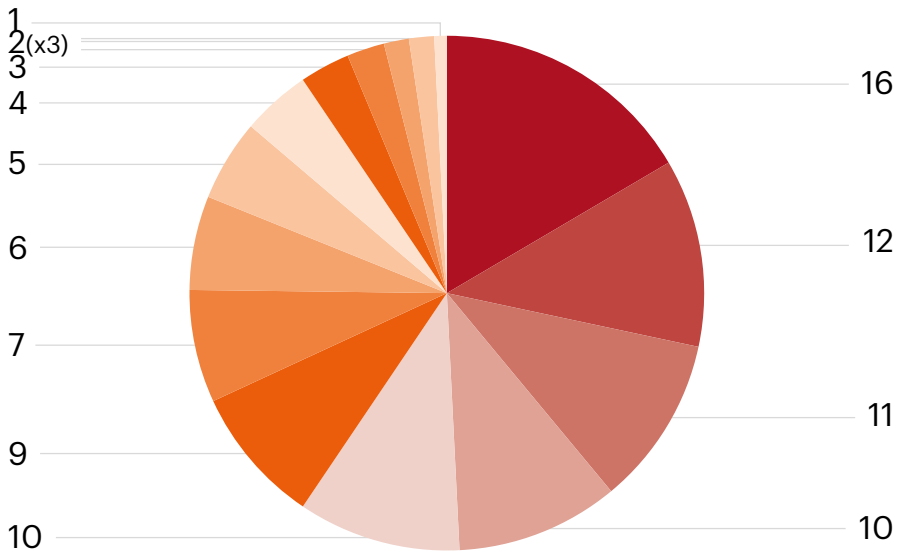


CHART 01
Industry sectors of participating organizations

Legend
Consolidated view
n = 254 separate companies

- Financial services
- Industrial/ manuf'ng.
- Services
- Tech and software
- Retail
- Public sector
- Utilities and energy
- Consumer products
- Healthcare
- Transportation
- Life science
- Hospitality
- Communications
- Education
- Aerospace and defense

Chart 2 shows the percentage frequency of companies based on the number of enterprise seats connected to networks or systems. Our analysis of cyber crime cost only pertains to organizations with a minimum of approximately 1,050 seats. In the 2017 global study, the largest number of enterprise seats exceeded 259,000.

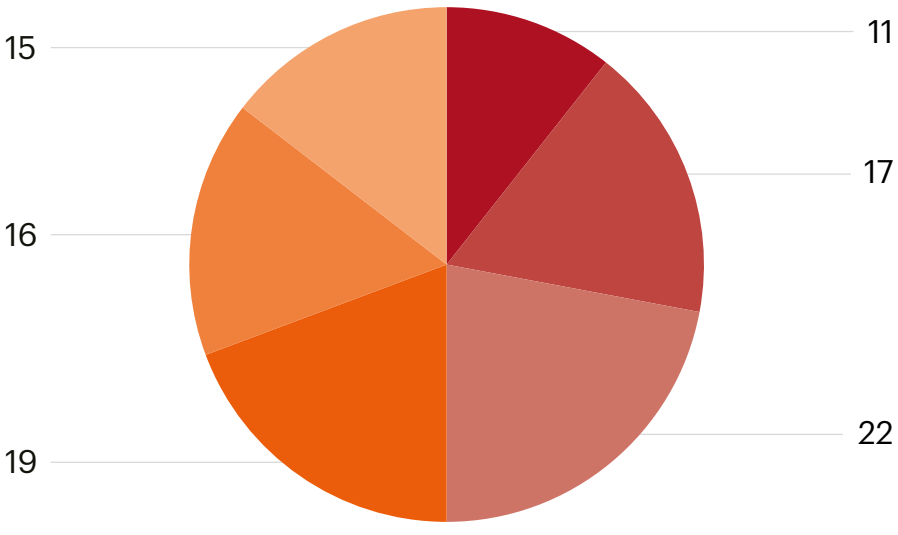


CHART 02
Distribution of participating organizations by enterprise seats (size)

Legend
Consolidated view
n = 254 separate companies

- < 2,000
- 2,000 to 5,000
- 5,001 to 10,000
- 10,001 to 15,000
- 15,001 to 25,000
- > 25,000

Limitations

This study utilizes a confidential and proprietary benchmark method that has been successfully deployed in earlier Ponemon Institute research. However, there are inherent limitations to benchmark research that need to be carefully considered before drawing conclusions from findings.

Non-statistical results

The purpose of this study is descriptive rather than normative inference. The current study draws upon a representative, non-statistical sample of organizations of mostly larger-sized entities experiencing one or more cyber attacks during a four-week fielding period. Statistical inferences, margins of error and confidence intervals cannot be applied to these data given the nature of our sampling plan.

Non-response

The current findings are based on a small representative sample of completed case studies. An initial mailing of benchmark surveys was sent to a targeted group of organizations, all believed to have experienced one or more cyber attacks. A total of 254 companies provided usable benchmark surveys. Non-response bias was not tested so it is always possible companies that did not participate are substantially different in terms of the methods used to manage the cyber crime containment and recovery process, as well as the underlying costs involved.

Sampling-frame bias

Because our sampling frame is judgmental, the quality of results is influenced by the degree to which the frame is representative of the population of companies being studied. It is our belief that the current sampling frame is biased toward companies with more mature information security programs.

Company-specific information

The benchmark information is sensitive and confidential. The current instrument does not capture company-identifying information. It also enables individuals to use categorical response variables to disclose demographic information about the company and industry category. Industry classification relies on self-reported results.

Unmeasured factors

To keep the survey concise and focused, we decided to omit other important variables from our analyses such as leading trends and organizational characteristics. The extent to which omitted variables might explain benchmark results cannot be estimated at this time.

Estimated cost results

The quality of survey research is based on the integrity of confidential responses received from companies. Checks and balances were incorporated into the survey process. In addition, the use of a cost estimation technique (termed shadow costing methods) rather than actual cost data could create significant bias in presented results.

CONTACT US

Kevin Richards
k.richards@accenture.com

Ryan LaSalle
ryan.m.lasalle@accenture.com

Matt Devost
matt.devost@accenture.com

Floris van den Dool
floris.van.den.dool@accenture.com

Josh Kennedy-White
j.kennedy-white@accenture.com

Ponemon Institute LLC
Attn: Research Department
2308 US 31 North
Traverse City, Michigan 49629 USA
1.800.887.3118
research@ponemon.org

Visit us at http://www.accenture.com

Follow us @AccentureSecure

Connect with us

The views and opinions expressed in this document are meant to stimulate thought and discussion. As each business has unique requirements and objectives, these ideas should not be viewed as professional advice with respect to your business.

This document makes descriptive reference to trademarks that may be owned by others. The use of such trademarks herein is not an assertion of ownership of such trademarks by Accenture and is not intended to represent or imply the existence of an association between Accenture and the lawful owners of such trademarks.

ABOUT ACCENTURE

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With approximately 411,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. Visit us at **www.accenture.com**

ABOUT ACCENTURE SECURITY

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organization's valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown. Follow us @AccentureSecure on Twitter or visit the Accenture Security blog.

ABOUT PONEMON INSTITUTE

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.